National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Biometrics "Foundation Documents"

Table of Contents

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Biometrics 'Foundation Documents'	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Science and Technology Council (NSTC),Committee on Technology,Subcommittee on Biometrics,Washington,DC,20502**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**167**	

Biometrics Frequently Asked Questions

Introduction

This set of Frequently Asked Questions (FAQs) was developed by the National Science & Technology Council's (NSTC) Subcommittee on Biometrics with the full understanding that national (INCITS/M1) and international (ISO/IEC JTC1 SC37) standards bodies are working to develop standard references. The subcommittee will review this set of FAQs for consistency as standards are passed. The subcommittee recognizes the impact of ongoing challenge problems, technical evaluations, and technology advancements. The FAQs will be updated accordingly to reflect these changes. The statements herein are intended to further the understanding of a general audience and are not intended to replace or compete with sources that may be more technically descriptive/prescriptive.

Top 10 Biometric FAQs

Q1: What is "biometrics"?

Biometrics is a general term used alternatively to describe a characteristic or a process.

- As a characteristic: a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
- As a process: a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Q2: What are the common biometrics?

Biometrics commonly implemented or studied include fingerprint, face, iris, voice, signature, and hand geometry. Many other modalities are in various stages of development and assessment.

Q3: Which biometric technology is the best?

There is not one biometric modality that is best for all implementations. Many factors must be taken into account when implementing a biometric device including location, security risks, task (identification or verification), expected

number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity. For example, fingerprint recognition has been used for over a century while iris recognition is a little more than a decade old. It should be noted that maturity is not related to which technology is the best, but can be an indicator of which technologies have more implementation experience.

Q4: How are biometrics collected?

Biometrics are typically collected using a device called a sensor. These sensors are used to acquire the data needed for recognition and to convert the data to a digital form. The quality of the sensor used has a significant impact on the recognition results. Example "sensors" could be digital cameras (for face recognition) or a telephone (for voice recognition).

Q5: What are biometric templates?

A biometric template is a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. Templates can vary between biometric modalities as well as vendors. Not all biometric devices are template based. For example, voice recognition is based on "models." The difference between templates and models is beyond the scope of this paper.

Q6: What is the difference between recognition, verification and identification?

- *Recognition* is a generic term, and does not necessarily imply either verification or identification. All biometric systems perform "recognition" to "again know" a person who has been previously enrolled.
- *Verification* is a task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.
- *Identification* is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a

"watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database.

Q7: Where are biometric technologies currently being deployed?

Biometrics are being used in many locations to enhance the security and convenience of the society. Example deployments within the United States Government include the FBI's IAFIS, the US-VISIT program, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program. These deployments are intended to strengthen the security and convenience in their respective environments. Many companies are also implementing biometric technologies to secure areas, maintain time records, and enhance user convenience. For example, for many years Disney World has employed biometric devices for season ticket holders to expedite and simplify the process of entering its parks.

Q8: Can I interact with a biometric device without touching something?

This depends on the specific modality being used. For example, with today's current technology, an individual would be required to touch a fingerprint sensor for the system to obtain the biometric sample, whereas face imaging for face recognition and iris imaging for iris recognition are contactless and would not require the user to touch the system.

Q9: Can I interact with a biometric device without touching something?

Biometrics is a security tool available for use. An environment or circumstance may or may not need a biometric system, depending on the application. To determine if a biometric is needed, one must understand the operational requirements of the situation. Biometrics should not be forced; each circumstance should be evaluated to determine the benefits that a biometric may provide.

Q10: What if my biometric does not work?

On any biometric system, secondary procedures need to be implemented. It is important to remember that biometrics are a component of an overall system architecture, and contingency plans will vary from application to application.

Background

Q: What are the different biometrics modalities and what are their advantages/disadvantages?

Fingerprint

Advantages

- Subjects have multiple fingers
- Easy to use, with some training
- Some systems require little space
- Large amounts of existing data to allow background and/or watchlist checks
- Has proven effective in many large scale systems over years of use
- Fingerprints are unique to each finger of each individual and the ridge arrangement remains permanent during one's lifetime

Disadvantages

- Public Perceptions
  - Privacy concerns of criminal implications
  - Health or societal concerns with touching a sensor used by countless individuals
- Collection of high quality nail-to-nail images requires training and skill, but current flat reader technology is very robust
- An individual's age and occupation may cause some sensors difficulty in capturing a complete and accurate fingerprint image

Iris

Advantages

- No contact required
- Protected internal organ; less prone to injury
- Believed to be highly stable over lifetime

Disadvantages

- Difficult to capture for some individuals

- Easily obscured by eyelashes, eyelids, lens and reflections from the cornea
- Public myths and fears related to "scanning" the eye with a light source
- Acquisition of an iris image requires more training and attentiveness than most biometrics
- Lack of existing data deters ability to use for background or watchlist checks
- Cannot be verified by a human

Face

Advantages

- No contact required
- Commonly available sensors (cameras)
- Large amounts of existing data to allow background and/or watchlist checks
- Easy for humans to verify results

Disadvantages

- Face can be obstructed by hair, glasses, hats, scarves, etc.
- Sensitive to changes in lighting, expression, and pose
- Faces change over time
- Propensity for users to provide poor-quality video images yet to expect accurate results

Hand Geometry

Advantages

- Easy to capture
- Believed to be a highly stable pattern over the adult lifespan

Disadvantages

- Use requires some training
- Not sufficiently distinctive for identification over large databases; usually used for verification of a claimed enrollment identity
- System requires a large amount of physical space

Speaker/Voice

Advantages

- Public acceptance
- No contact required
- Commonly available sensors (telephones, microphones)

Disadvantages

- Difficult to control sensor and channel variances that significantly impact capabilities
- Not sufficiently distinctive for identification over large databases

Others

Many other biometric modalities exist and are in various stages of research or commercialization. Examples include gait (the manner of walking), retina and other vascular pattern recognition, ear structure, odor, and palm prints.

Q: Why are there so many different biometric modalities?

Different applications and environments have different constraints. For instance, adequate fingerprint samples require user cooperation; whereas, a face image can be captured by a surveillance camera. Furthermore, fingerprints are not available for many of the suspects on watchlists. There are also multiple biometric modalities for technical and financial reasons. Many scientists become interested in developing a system based on their own research. Upon a successful implementation, venture capitalist, interested in the implementation of such a system, commercialize a product. Therefore, wide varieties of modalities are being researched and are available on the market.

Q: Can I change my biometrics?

Biological biometrics cannot easily be changed (there have been cases of mutilated or surgically altered fingerprints), but they can be disguised. It may be possible to change a behavioral biometric.

Q: What if identical twins use a biometric device?

Although identical twins may appear the same to the human eye, their biological and behavioral characteristics

are usually subtly different. The automated methods implemented in some biometric devices can often identify such differences and differentiate between two seemingly identical twins.

Q: Are biometrics safe to use?

Biometrics are typically passive and designed to be safe to use. Biometric systems usually implement ordinary computing and video technology, such as that encountered in a person's day-to-day activities.

Q: Are biometrics a new idea?

No, methods of recognizing humans have existed for centuries. The most obvious example is the human use of face recognition. Also, handprints were discovered surrounding cave paintings, estimated to be 31,000 years old, and are believed to be the artists' signatures. However, the means for automating such identification is fairly new, dating only to the early 1960s. Automation recognition became possible within the last few decades with the advancement of computer processing capabilities. The individual biometric modalities vary in their stages of maturity. Fingerprint began the transition to automation in the late 1960s, while iris is a little over a decade old. Many methods, such as gait, are still in the research and development stage and are not yet ready for deployment.

Q: Are biometrics intrusive?

This is a subjective question that would be answered differently by various individuals. In general, most biometrics are non-intrusive, requiring only the placement of a finger, a look in the proper direction, or a statement to be said aloud.

Q: Are biometric systems difficult to use?

This question is subjective and depends on each individual. Those users more familiar with electronics technology tend to have fewer issues than those who are not familiar or are skeptical about using technology. From the operational perspective, most people are able to use a biometric system with very little training.

Once I register my biometric, will that registration be good anywhere that specific technology is used?

In general, no. A biometric registered on one system will typically not be valid for another system on which that

biometric might be used. However, if the system on which the biometric was registered is connected to another system, e.g. via a network, then yes, a biometric could also be accepted at the alternate system location.

Q: What is the difference between biometrics and forensics?

While both biometrics and forensics involve human recognition, biometrics is typically applied using automated techniques to the pre-event situation application, such as gaining access to sensitive information or to a secured facility. Forensic applications typically occur after a crime has occurred, and may not use fully automated methods. Forensic methods are often used to assist in the adjudication (legal) process. Forensics usually requires days of processing (versus seconds for biometrics) and are held to much higher accuracy requirements.

Q: What is biometric authentication?

"Biometric authentication" is a generic term for the process of verification. It involves presenting a biometric for query, comparing the presented biometric to a stored template or model, and determining whether the individual has made a legitimate claim.

Q: Do biometric features remain constant over time?

The permanence of biometrics varies between modalities. For instance, fingerprints remain constant over one's lifespan, except for surface wear degrading the prominence and definition of the ridges. Fingerprints are based on physical dermal structures that are defined during fetal development. Temporary or permanent scarring can affect the original fingerprint patterns developed before birth. Aging affects faces more dramatically. Detailed studies of the effects of aging on other modalities have not yet been performed.

Q: What factors contribute to the development of a person's biometric?

A biometric is first affected by the individual's unique genetic makeup. An individual's biometric is also affected by the individual's environment. For example, characteristics such as fingerprints and iris structures are affected by the environmental factors encountered by a fetus in the prenatal environment.

Q: How do biometric systems determine "matches"?

Biometric systems can be described, albeit in an over-simplified manner, by a three-step process. The first step in this process involves an observation, or collection, of the biometric data. This step uses various sensors, which vary between modality, to facilitate the observation. The second step converts and describes the observed data using a digital representation called a template. This step varies between modalities and also between vendors. In the third step, the newly acquired template is compared with one or more templates stored in the database. The results of this comparison are a "match" or a "non-match" and are used for actions such as permitting access, sounding an alarm, etc.

Implementation

Q: What are the common uses of biometrics?

Common examples of biometric use involve controlling access to physical locations (laboratories, buildings, etc.) or logical information (personal computer accounts, secure electronic documents, etc). Biometrics can also be used to determine whether or not a person is already in a database, such as for social service or national ID applications.

Q: Where can biometrics be used?

Biometrics can be used in environments where recognition of an individual is required. Applications vary and range from logical access to a personal computer, to physical access of a secure laboratory. They can be used in a variety of collection environments as identification systems. Biometrics are also used for accountability applications, such as recording the biometric identities of individuals boarding an aircraft, signing for a piece of equipment, or recording the chain of evidence. Of course, biometrics perform more reliably in controlled environments, such as offices and laboratories, than in uncontrolled environments, such as outdoors.

Q: Where/How would biometric verification be used?

Verification is used where it is necessary to confirm that an individual is enrolled in a database with the authorizations claimed. In this case, an individual would present a

biometric to the system and the system would either verify or not verify that the person is who he or she claimed to be. For example, biometric verification can be used to regulate gaining physical or logical access or for accountability monitoring.

Q: Where/How would biometric identification be used?

Identification is used when the need arises to determine whether or not a person is in a database, absent a claim of identity. In this case, an individual would present his/her biometric to the system and the system would either provide the identity of the person or indicate that the person is not represented in the system. For example, the FBI uses identification methods in its search of fingerprints to determine whether the fingerprint indicates connection to a record of a known person. Another possible application involves using face recognition technology to identify abducted children in a public area or on the Internet.

Q: What are the goals of biometric standards?

Technology standards enable development of integrated, scalable and robust solutions and cut down the cost of development and maintenance of system solutions. Biometric standards have been and are currently being developed on both the national and international levels. Organizations at the national and international levels are focusing on creating a standard set of biometric data interchange definitions, developing standards to promote interoperability between various systems, creating standards for testing biometrics and for testing conformance to biometric standards. According to NIST (NISTIR 6529), standards should be technology neutral and not favor any particular vendor or modality.

Q: What benefits/cost savings will biometrics provide?

The usefulness of biometrics varies from application to application. To determine its true benefit, one must first develop and understand the operational requirements of the application. Biometrics can provide an automated means for identification of an individual or verification of a claimed identity. Before making a decision, one must ensure this task will meet the determined operational needs. Biometrics can potentially provide cost savings through relocating security resources or diminishing the

expenses associated with password maintenance, or it could cause extra costs by highlighting problems that were previously missed. The cost benefits vary from application to application as well.

Q: How do I select a biometric technology?

The effectiveness of a biometric technology is dependent on the how and where it is used. Each biometric modality has its own strengths and weaknesses that should be evaluated in relation to the application before implementation. Key decision factors for selecting a biometric technology include evaluating the environment, throughput needs, population size and demographics, ergonomics, interoperability with existing systems, user considerations, etc. For instance, an access control system to a coal mine, where individuals will have very worn and dirty fingerprints, will not be a suitable environment for a fingerprint reader. The careful evaluation of the key decision factors plays a crucial role in the success of the selected technology.

Q: Can everyone be enrolled? If not, then what?

There are some instances when an individual may not have characteristics that are of sufficient quality to enable enrollment in a biometric system. The probability of such instances is small in most application environments, although it is important to have a contingency plan when such failures to enroll occur.

Q: Will biometrics solve all of the security problems?

No, biometrics should be one part of an overall security system implementation plan. A biometric system alone cannot solve a security problem.

Q: How fast does a biometric system work?

This will vary from application to application. It will depend on the hardware and software implemented, user training, the environmental application, and whether human involvement is required in some or all cases to make final decisions. For example, to complete a civil fingerprint background check, the average processing time is approximately 24 hours. On the other hand, implementing fingerprint verification in an airport may be completed in under a second.

Q: Many access control situations make use of a smart card in addition to a biometric. Why is this necessary?

There are three ways to identify someone: by what they have (a token, e.g. a smart card), by what they know (a pin or password) and by what they are (a biometric). The use of a smart card and a biometric adds a level of security to the system. It incorporates both what they "have" (the smart card) and what they "are" (the biometric). The smart card is often also used to claim an identity for the biometric system to verify. The smart card may contain information (such as cryptographic keys) that may require a biometric for use.

Q: What are the components of a biometric system?

A typical biometric system is comprised of five integrated components. A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps information that new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process (either automated or human-assisted) uses the results from the matching component to make a system-level decision.

Q: What are the processes of a biometric system?

Biometrics systems follow four basic processes: collection, extraction, comparison, and decision. Collection involves using a sensor to capture the biometric traits and convert them to a digital format. Extraction takes the digital data and converts the distinctive features into a compact template. In the comparison step, the biometric system measures the likeness of the template to those in the database. Based on the likeness, the system decides whether or not the submitted biometric matches one of the templates in the database.

Q: Can biometrics be integrated into an existing system?

In general, yes, biometrics can be integrated into existing systems. Like all technologies, however, it is sometimes difficult to integrate biometrics as "retrofits" with existing systems if they weren't designed to accept newer techniques.

Q: Are biometrics going to affect the time required to do things (e.g. clear airport security, access a secure building)?

Biometric systems may or may not affect the time required depending on the application and the design of both the old and new systems. It is based on the efficiency of the current process. For example: identification at a choke point, if implemented correctly, will not affect the time; DHS' Registered Traveler (RT) program, where individuals have been processed and trusted prior to verification, will decrease the time; and the addition of a system in a location where a system did not previously exist will increase the time.

Q: What factors cause biometric systems to fail?

In addition to common electronics/computer and hardware failures, common biometric issues include poor-quality biometric samples, user confusion, evasion or non-cooperation, noise, inadequate or excessive lighting, dirty sensor, or subject handicaps.

Q: How do you know biometric technology will work as expected?

A properly designed implementation plan involves a series of evaluations, first focusing on algorithm accuracy (technology evaluation), then assessing performance in a mock environment (scenario evaluation), followed by live testing on site (operational evaluation) before full operations begin. If done properly, users will know, to a high degree of accuracy, how the system will perform.

Personal Concerns

Q: How do you know biometric technology is safe (healthy) to use?

Most biometric systems use everyday sensors, such as a digital camera, to obtain the observations of an individual's biometric; other sensors would need to be analyzed. Most stated health concerns are actually similar to those encountered in everyday life (touching a fingerprint sensor is roughly equivalent to touching a doorknob).

Q: Can biometrics reveal private information (medical information, drug use, ethnicity, disease detection, etc.)?

Biometric systems cannot detect diseases; however, some of the information gathered using some biometric modalities could potentially be used to detect medical information or drug use. These diagnoses require specialized training, however. The image data from a face recognition system may allude to the individual's ethnicity.

Q: Do biometrics invade an individual's civil liberties and privacy?

Many US Supreme Court findings (e.g. Schmerber v. CA.,384 U.S. 757, 1966; U.S. v Dionisio, 410 U.S. 1, 1973) imply that the use of biometrics does not invade an individual's civil liberties or privacy, although personal viewpoints are subjective and may differ. A well thought through biometric system implementation should be considerate of these issues.

Q: If I provide my biometric, who has access to it (and the information associated with it)?

Access to biometrics stored within the system is a system implementation issue, not a biometrics issue. Each system will be different, and it is recommended that an individual be aware of the use and access to his/her biometrics before providing a biometric to a system.

Q: Can someone steal my biometric(s)?

Although it may be possible to steal one's biometric for use with certain modalities, for example cutting off one's finger or creating a synthetic model of a fingerprint or iris pattern, it is not a practical or realistic concern in most applications. Many vendors are working actively on "liveness" detection mechanisms for determining if a living person is indeed presenting the sample. Although this does not prevent "stealing" of a biometric in all applications, it is an important element in overall system security. In important United States government applications, such as US-VISIT, the biometric is captured in the presence of an immigration officer, who can detect the presence of a forgery. It is important to note that once the system digitizes the biometric data, it faces the same vulnerabilities faced by typical (non-biometric) computer systems.

Q: What happens if I am enrolled in a fingerprint system and I cut my finger?

Minor scrapes typically do not impact a biometric system. Severe injuries would require a re-enrollment of the healed finger or the enrollment of a different finger. Some biometric systems allow for the enrollment of a secondary sample. For instance, an individual may be able to use his or her left index finger for verification purposes in the event he or she has injured the right index finger.

Performance Statistics

Q: Is there an advantage in combining multiple biometrics?

There is a potential for advancement in some applications if the combination is implemented properly. Combining biometrics incorrectly would result in performance less than that of a single measure.

Q: Is failure to enroll a problem with biometrics?

There are some instances when an individual may not be able to provide an image of sufficient quality to the biometric system. For instance, a fingerprint may not be rolled correctly or there may be dirt on the sensor. Iris technologies are tuned to accept good quality images only. Individual disabilities may exist, such as lacking a finger. The probability of most of these instances is fairly small, but each implementation should have contingency plans in place.

Q: Is the biometric system accuracy dependent on the user?

Yes, to some degree. Some individual users may find using certain modalities more difficult than other users.

Q: How reliable/accurate are biometrics?

Biometric technology is continually improving. The latest government evaluations are available in the Biometrics Catalog, http://www.biometricscatalog.org.

Q: Do biometric matches provide a 100% guarantee?

No technology can provide a 100% guarantee. The key is to determine where the system will be successful and how to implement it correctly for the application. For example, a metal detector must have correct placement and sensitivity

adjustments to work effectively and appropriately; the same is true of a biometric system.

Q: What are the performance metrics (FRR, FAR, TAR, TRR, FTE, etc.)?

Performance metrics require more discussion than this forum allows. Please refer to http://www.biometricscatalog.org/biometrics/biometrics_101.pdf for a detailed description of performance metrics.

Q: How is the accuracy of a biometric system measured?

The accuracy of a biometric system is determined through a series of tests beginning with an assessment of matching algorithm accuracy (technology evaluation), then assessing performance in a mock environment (scenario evaluation), followed by live testing on site (operational evaluation) before full operations begin. If done properly, users will know, to a high degree of accuracy, how the system will perform.

Q: What is a threshold?

A value, predefined by the system administrator or the device producer, which is used to establish the degree of correlation between the biometric provided and the stored template that will result in a match.

Security

Q: Are biometrics more secure than passwords?

In general, security of a system depends on the design of that system and its operational implementation. In general, a properly designed biometric system would be more secure than a properly designed password system because the system is inherently harder to spoof.

Q: Could someone use a replica of the user's biometric to gain unauthorized access to the system?

In rare instances, it may be possible. Although this a question frequently asked, it is more science fiction than a reality. In reality, it is much easier to find alternative weaknesses to a system than to mimic the biometric of a genuine user.

Q: How do performance metrics affect security (e.g. as the FAR decreases, does the security increase)?

There is a trade-off with the relative errors; false acceptance rates generally increasing as false rejection rates decrease. Performance measures, such as a Receiver Operating Characteristics (ROC) curve, highlight the accuracy of a system in a specific instance. This information can be used to maximize the security and convenience based on the needs of the specific application.

Q: Can a biometric be reconstructed from a template?

There have been studies where pseudo-fingerprint images have been reconstructed from the fingerprint template, and face images have been reconstructed from face templates. In these instances, it is essential that specific information about the enrollment process is known.

Q: What is liveness detection?

Liveness detection is used to ensure that only characteristics from a living human being can be enrolled, stored and recognized in a biometric system. Liveness detection can be used to recognize spoof attacks (e.g. submission of a fake biometric sample.)

Q: What happens when a biometric is compromised (stolen)?

Biometrics are one part of an overall system. Actions taken when a system is compromised will vary from system to system.

Q: What is skimming?

The act of obtaining data from an unknowing end user that is not willingly submitting the sample at that time. An example could be secretly reading data while in close proximity to a user on a bus.

Q: What is eavesdropping?

Surreptitiously obtaining data from an unknowing end user that is performing a legitimate function. An example involves having a hidden sensor co-located with the legitimate sensor.

Modality Specific

Fingerprint

Q: What are slap fingerprints (slaps)?

Slaps are fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card. Slaps are known as four finger simultaneous plain impressions.

Q: How many fingerprints are best?

The number of fingerprints required is application dependent based on the implementation details. While a single fingerprint might prove sufficiently accurate for certain applications, two fingerprints may be required for increased levels of accuracy. In general, ten rolled fingerprints will always have the potential for the highest accuracy, but they take much more time to gather with the current capture technology.

Q: Are fingerprints inherited? Are they more similar between family members than between strangers?

Close relatives may have similar patterns, such as loops, whorls, or arches. This information is typically not used directly for recognition. The minutiae pattern, which is used for recognition, is not inherited or similar; this characteristic even differs between an individual's own fingers and the fingers of identical twins.

Q: Can children's fingerprints be collected?

Yes, in most cases, a child's fingerprints can be collected after the age of one year or so, but the prints may not have the clarity of adult prints. It is not clear whether fingerprints taken from children can be automatically matched to those same individuals later as adults.

Q: What is a "latent fingerprint"?

A latent fingerprint is a fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger.

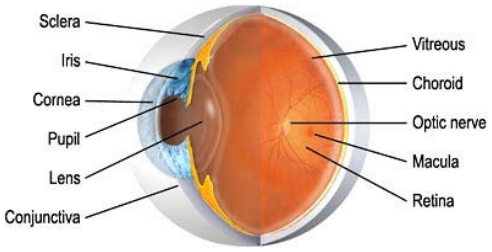
Q: If a latent print is acquired, can it be used to access a biometric system?

Theoretically, yes, some latent prints could potentially be used to gain access to a system implementing biometrics, but it is not a practical or cost-effective approach in most applications. There are easier ways to break into a system. Many systems are implementing liveness detection to prevent attacks such as this from occurring.

Iris/Retina

Q: What is the difference between iris and retina recognition?

Iris recognition uses the unique patterns in the individual's iris, a muscle that is the colored portion on the front of the eye. Retinal recognition uses the unique pattern of blood vessels on an individual's retina at the back of the eye.



[Source: http://www.stlukeseye.com/Anatomy.asp]

Q: Is iris or retina recognition dangerous to the eye?

Iris and retina recognition involve capturing a high quality picture of the iris or retina, using a digital camera. In the acquisition of these images, some form of illumination is necessary. Iris uses near infrared light, which is believed to be safe. Although retina technology is not currently available, previous technology involved the illumination of the retina using infrared and visible light. Literature is inconclusive on the long-term effects of repetitive exposure to this illumination.

Q: Does iris or retina recognition use a laser?

No, neither iris nor retinal recognition makes use of a laser. Both techniques use some form of illumination, but these techniques are not lasers as the term is commonly understood.

Q: What is the impact of contact lenses on iris recognition systems?

Typically, contacts do not affect the performance of the system, although some color changing and patterned contacts haven proven to be an issue. Also, some issues have occurred in the recognition of individuals wearing hard gas permeable contacts.

Q: Can iris recognition be used for identification purposes?

Yes, it is possible to use iris for identification.

Face

Q: What effects will facial expressions, hairstyle, glasses, hats, makeup, etc. have on face recognition systems?

Minor variances, such as those mentioned, will have a moderate impact on a face recognition system, decreasing its ability to recognize faces. The proposed ISO standard for facial recognition (ISO 19794-5) requires the removal of dark glasses and hats, movement of the hair away from the eyes, and recommends a neutral facial expression. Anything that sufficiently obscures the primary face region will have a negative impact on the recognition system.

Other

Q: What is the difference between speech and speaker recognition?

Speech recognition is the identification of the words being said, and is not a biometric technology. Speaker recognition (sometimes referred to as voice recognition) recognizes the speaker, not the words. Speaker recognition is a biometric technology.

Q: Is speaker recognition language/word independent?

Word independent speaker recognition systems are available and can be used in any language. Whether or not speakers can be recognized if they change languages is the subject of current testing.

Q: What is a behavioral biometric?

A behavioral biometric is one based on an individual's unique actions and is captured over a period of time.

Examples are gait (the way an individual walks), keystroke dynamics, and signature dynamics.

Q: Is DNA a biometric?

There is not universal agreement on this issue. At this point, DNA recognition is not performed by an automated method, and is therefore not considered a biometric; however, it may be at some point in the future.

Q: Is Radio Frequency Identification (RFID) a biometric?

No, RFID is a technology that may be integrated with biometrics. Unlike biometrics, RFID systems are not biologically tied to an individual. RFID is a technology that stores and retrieves data remotely through devices called RFID tags or transponders. These devices use radio frequency (RF) signals to exchange information. They contain antennas that allow them to respond to queries from RFID transceivers. Some examples of RFID tags include sensors in library books, E-PASS Toll Collectors, and building access control cards.

Government Specific

Q: What actions are being taken to ensure stored biometrics data isn't compromised?

Biometric data is considered sensitive personal information collected by the government and is thus subject to the same laws, regulations, and standards.

Q: What government agencies are researching or working with biometrics?

Many government agencies are working with biometrics. Specifically, the government is implementing the PIV (Personal Identity Verification) Program to issue identity cards with biometrics for all Federal employees and contractors. Federal agencies are also developing and implementing biometrics to meet other operational needs. The National Science and Technology Council (NSTC) is working to coordinate high priority activities within these agencies.

http://www.biometricscatalog.org/NSTCSubcommittee/default.asp

Q: How accurate are the two fingerprint scans used in US-VISIT?

Actual operational accuracy of the US-VISIT system is sensitive. Data on the basic performance of US-VISIT algorithms is available at ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7110.pdf. General information regarding the accuracy of commercial fingerprint systems can be found in FpVTE 2003 http://fpvte.nist.gov/.

Q: With regard to domestic and foreign travel, how are biometrics collected at various United States government facilities?

For most foreign visitors to the United States, the DHS's US-VISIT program captures a photograph and two flat fingerprint images that are stored in its IDENT database. Currently, United States citizens are not required to supply biometric data when crossing the borders into or out of the United States.

Q: Are biometrics obtained on everyone that enters or exits the United States?

Biometrics are collected from most foreign visitors entering the United States, but not from United States citizens.

Q: Who has access to the information in government biometric databases?

Personal information access is limited to those individuals who have a "need to know," according to law, to protect United States Government operations.

Q: Which modalities do the Department of "X" use, or plan to use, in the future?

Most departments use a variety of biometric modalities selected based on the needs of the specific applications. These departments are continually re-accessing the uses to determine the method that is in the best interest for maximizing security and prosperity of the country.

Q: Will there be a government-wide standard biometric?

Because no modality is suitable for all applications, there will not be a universal biometric for government use.

Q: Some fingerprint systems use 10 prints, other fingerprint systems use two; some fingerprint systems use rolled

fingerprints and other fingerprint systems use flat fingerprints. Why?

The various collection methods are used to meet a combination of operational needs, current capabilities, cost, and legacy systems. In general, the more quality data one has, the greater precision available; however, more data requires more storage, processing power, etc.

Biometrics Glossary

Introduction

This set of terms was developed by the National Science & Technology Council's (NSTC) Subcommittee on Biometrics with the full understanding that national (INCITS/M1) and international (ISO/IEC JTC1 SC37) standards bodies are working to develop standard references. The subcommittee will review this Glossary for consistency as standards are passed. The subcommittee recognizes the impact of ongoing challenge problems, technical evaluations, and technology advancements. The Glossary will be updated accordingly to reflect these changes. The statements herein are intended to further the understanding of a general audience and are not intended to replace or compete with sources that may be more technically descriptive/prescriptive.

Glossary Terms

Accuracy

A catch-all phrase for describing how well a biometric system performs. The actual statistic for performance will vary by task (verification, open-set identification (watchlist), and closed-set identification). See http://www.biometricscatalog.org/biometrics/biometrics_101.pdf for further explanation. *See also d prime, detection error trade-off (DET), detect and identification rate, equal error rate, false acceptance rate (FAR), false alarm rate (FAR), false match rate, false non-match rate, false reject rate, identification rate, performance, verification rate.*

Algorithm

A limited sequence of instructions or steps that tells a computer system how to solve a particular problem. A biometric system will have multiple algorithms, for example: image processing, template generation, comparisons, etc.

ANSI - American National Standards Institute

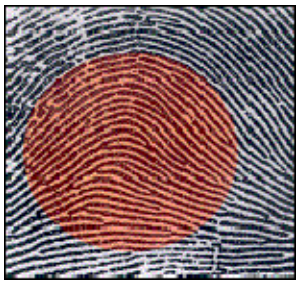
A private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. The mission of ANSI is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity. For more information visit http://www.ansi.org/. *See also INCITS, ISO, NIST.*

Application Programming Interface (API)

Formatting instructions or tools used by an application developer to link and build hardware or software applications.

Arch

A fingerprint pattern in which the friction ridges enter from one side, make a rise in the center, and exit on the opposite side. The pattern will contain no true delta point. *See also delta point, loop, whorl.*



Attempt

The submission of a single set of biometric sample to a biometric system for identification or verification. Some biometric systems permit more than one attempt to identify or verify an individual. *See also biometric sample, identification, verification.*

Authentication

1. The process of establishing confidence in the truth of some claim. The claim could be any declarative statement for example: "This individual's name is 'Joseph K.' " or "This child is more than 5 feet tall."
2. In biometrics, "authentication" is sometimes used as a generic synonym for verification. *See also verification.*

Automated Biometric Identification System (ABIS)

1. Department of Defense (DOD) system implemented to improve the U.S. government's ability to track and identify national security threats. The system includes mandatory collection of ten rolled fingerprints, a minimum of five mug shots from varying angles, and an oral swab to collect DNA.
2. Generic term sometimes used in the biometrics community to discuss a biometric system. *See also AFIS.*

Automated Fingerprint Identification System (AFIS)

A highly specialized biometric system that compares a submitted fingerprint record (usually of multiple fingers) to a database of records, to determine the identity of an individual. AFIS is predominantly used for law enforcement, but is also being used for civil applications (e.g. background checks for soccer coaches, etc). *See also IAFIS.*

Behavioral Biometric Characteristic

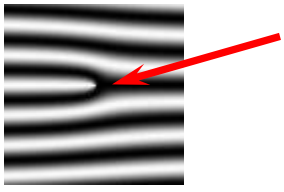
A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics. *See also biological biometric characteristic.*

Benchmarking

The process of comparing measured performance against a standard, openly available, reference.

Bifurcation

The point in a fingerprint where a friction ridge divides or splits to form two ridges, as illustrated below. *See also friction ridge, minutia(e) point, ridge ending.*



Binning

Process of parsing (examining) or classifying data in order to accelerate and/or improve biometric matching.

BioAPI – Biometrics Application Programming Interface

Defines the application programming interface and service provider interface for a standard biometric technology interface. The BioAPI enables biometric devices to be easily installed, integrated or swapped within the overall system architecture.

Biological Biometric Characteristic

A biometric characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry. *See also* *behavioral biometric characteristic*.

Biometrics

A general term used alternatively to describe a characteristic or a process.

As a characteristic:

> A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.

As a process:

> Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Biometric Consortium (BC)

An open forum to share information throughout government, industry, and academia. For more information visit http://www.biometrics.org.

Biometric Data

A catch-all phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrollment, verification, or identification process, but does not apply to end user information such as user name, demographic information and authorizations.

Biometric Sample

Information or computer data obtained from a biometric sensor device. Examples are images of a face or fingerprint.

Biometric System

Multiple individual components (such as sensor, matching algorithm, and result display) that combine to make a fully operational system. A biometric system is an automated system capable of:

1. Capturing a biometric sample from an end user
2. Extracting and processing the biometric data from that sample
3. Storing the extracted information in a database
4. Comparing the biometric data with data contained in one or more reference references
5. Deciding how well they match and indicating whether or not an identification or verification of identity has been achieved.

A biometric system may be a component of a larger system.

Capture

The process of collecting a biometric sample from an individual via a sensor. *See also* *submission*.

CBEFF - Common Biometric Exchange File Format

A standard that provides the ability for a system to identify, and interface with, multiple biometric systems, and to exchange data between system components.

Challenge Response

A method used to confirm the presence of a person by eliciting direct responses from the individual. Responses can be either voluntary or involuntary. In a voluntary response, the end user will consciously react to something that the system presents. In an involuntary response, the end user's body automatically responds to a stimulus. A challenge response can be used to protect the system against attacks. *See also liveness detection.*

Claim of identity

A statement that a person is or is not the source of a reference in a database. Claims can be positive (I am in the database), negative (I am not in the database) or specific (I am end user 123 in the database).

Closed-set Identification

A biometric task where an unidentified individual is known to be in the database and the system attempts to determine his/her identity. Performance is measured by the frequency with which the individual appears in the system's top rank (or top 5, 10, etc.). *See also identification, open-set identification.*

Comparison

Process of comparing a biometric reference with a previously stored reference or references in order to make an identification or verification decision. *See also match.*

Cooperative User

An individual that willingly provides his/her biometric to the biometric system for capture. Example: A worker submits his/her biometric to clock in and out of work. *See also indifferent user, non-cooperative user, uncooperative user.*

Core Point

The "center(s)" of a fingerprint. In a whorl pattern, the core point is found in the middle of the spiral/circles. In a loop pattern, the core point is found in the top region of the innermost loop. More technically, a core point is defined as the topmost point on the

innermost upwardly curving friction ridgeline. A fingerprint may have multiple cores or no cores. *See also arch, delta point, friction ridge, loop, whorl.*

Covert

An instance in which biometric samples are being collected at a location that is not known to bystanders. An example of a covert environment might involve an airport checkpoint where face images of passengers are captured and compared to a watchlist without their knowledge. *See also non-cooperative user, overt.*

Crossover Error Rate (CER)

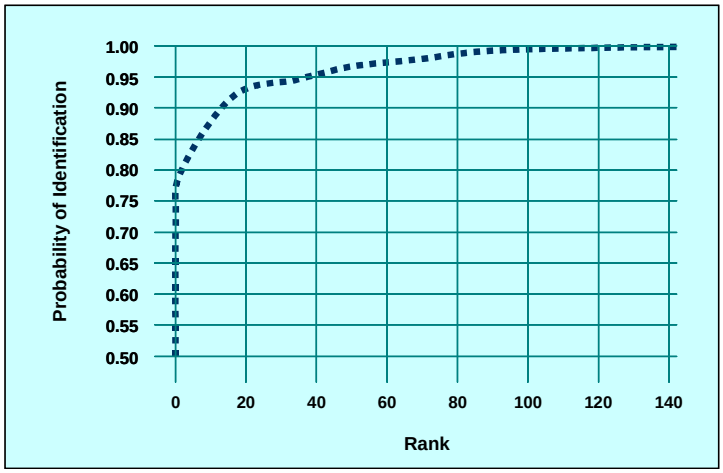
See equal error rate (EER).

Cumulative Match Characteristic (CMC)

A method of showing measured accuracy performance of a biometric system operating in the closed-set identification task. Templates are compared and ranked based on their similarity. The CMC shows how often the individual's template appears in the ranks (1, 5, 10, 100, etc.), based on the match rate. A CMC

compares the rank (1, 5, 10, 100, etc.) versus identification rate as illustrated below.

Cumulative Match Characteristic



D-Prime (D')

A statistical measure of how well a system can discriminate between a signal and a non-signal.

Database

A collection of one or more computer files. For biometric systems, these files could consist of biometric sensor readings, templates, match results, related end user information, etc. *See also gallery.*

Decision

The resultant action taken (either automated or manual) based on a comparison of a similarity score (or similar measure) and the system's threshold. *See also comparison, similarity score, threshold.*

Degrees of Freedom

A statistical measure of how unique biometric data is. Technically, it is the number of statistically independent features (parameters) contained in biometric data.

Delta Point

Part of a fingerprint pattern that looks similar to the Greek letter delta ( ), as illustrated below. Technically, it is the point on a friction ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence. *See also core point, friction ridge.*

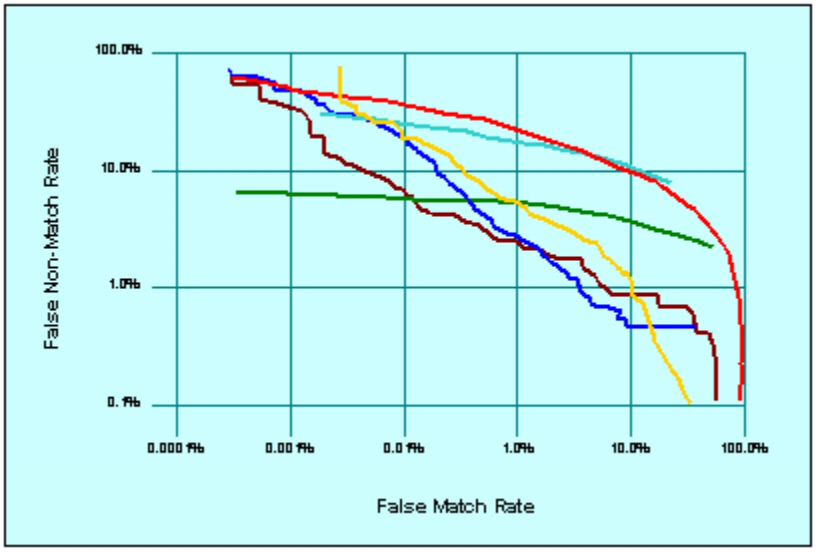
Detection and Identification Rate

The rate at which individuals, who are in a database, are properly identified in an open-set identification (watchlist) application. *See also open-set identification, watchlist.*

Detection Error Trade-off (DET) Curve

A graphical plot of measured error rates, as illustrated below. DET curves typically plot matching error rates (false non-match rate vs. false match rate) or decision error rates (false reject rate vs. false accept rate). *See also Receiver Operating Characteristics.*

Detection Error Trade-off (DET) Curve



Difference Score

A value returned by a biometric algorithm that indicates the degree of difference between a biometric sample and a reference. *See also hamming distance, similarity score.*

Eavesdropping

Surreptitiously obtaining data from an unknowing end user who is performing a legitimate function. An example involves having a hidden sensor co-located with the legitimate sensor. *See also skimming.*

EFTS - Electronic Fingerprint Transmission Specification

A document that specifies requirements to which agencies must adhere to communicate electronically with the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS). This specification facilitates information sharing and eliminates the delays associated with fingerprint cards. *See also Integrated Automated Fingerprint Identification System (IAFIS).*

Encryption

The act of transforming data into an unintelligible form so that it cannot be read by unauthorized individuals. A key or a password is used to decrypt (decode) the encrypted data.

End User

The individual who will interact with the system to enroll, to verify, or to identify. *See also cooperative user, indifferent user, non-cooperative user, uncooperative user, user.*

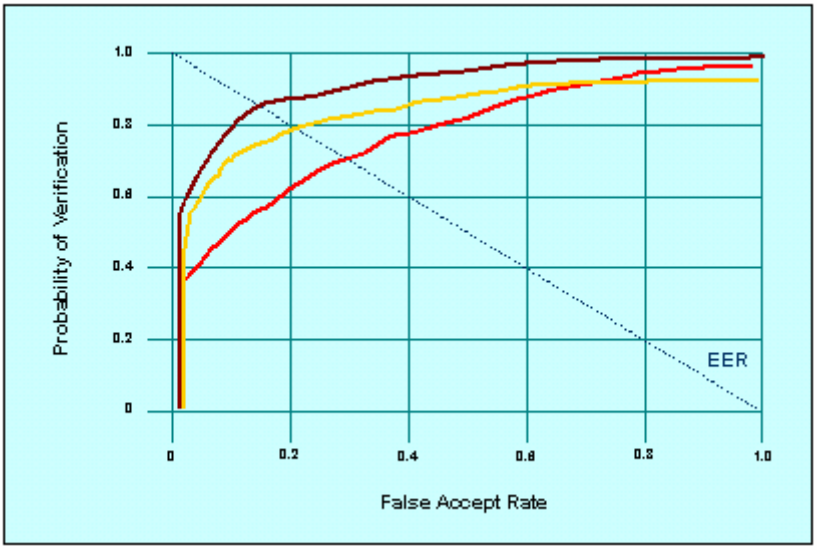
Enrollment

The process of collecting a biometric sample from an end user, converting it into a biometric reference, and storing it in the biometric system's database for later comparison.

Equal Error Rate (EER)

A statistic used to show biometric performance, typically when operating in the verification task. The EER is the location on a ROC or DET curve where the false accept rate and false reject rate (or one minus the verification rate {1-VR}) are equal, as illustrated below. In general, the lower the equal error rate value, the higher the accuracy of the biometric system. Note, however, that most operational systems are not set to operate at the "equal error rate" so the measure's true usefulness is limited to comparing biometric system performance. The EER is sometimes referred to as the "Crossover Error Rate." *See also* *Detection Error Trade-off (DET) curve*, *false accept rate*, *false reject rate*, *Receiver Operating Characteristics (ROC)*.

Receiver Operating Characteristic (ROC) Curves with Equal Error Rate



Extraction

The process of converting a captured biometric sample into biometric data so that it can be compared to a reference. *See also* *biometric sample*, *feature*, *template*.

Face Recognition

A biometric modality that uses an image of the visible physical structure of an individual's face for recognition purposes.

Failure to Acquire (FTA)

Failure of a biometric system to capture and/or extract usable information from a biometric sample.

Failure to Enroll (FTE)

Failure of a biometric system to form a proper enrollment reference for an end user. Common failures include end users who are not properly trained to provide their biometrics, the sensor not capturing information correctly, or captured sensor data of insufficient quality to develop a template.

False Acceptance Rate (FAR)

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometric. Example: Frank claims to be John and the system verifies the claim. *See also false match rate, type II error.*

False Alarm Rate

A statistic used to measure biometric performance when operating in the open-set identification (sometimes referred to as watchlist) task. This is the percentage of times an alarm is incorrectly sounded on an individual who is not in the biometric system's database (the system alarms on Frank when Frank isn't in the database), or an alarm is sounded but the wrong person is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

False Match Rate

A statistic used to measure biometric performance when. Similar to the False Acceptance Rate (FAR).

False Non-Match Rate

A statistic used to measure biometric performance. Similar to the False Reject Rate (FRR), except the FRR includes the Failure To Acquire error rate and the False Non-Match Rate does not.

False Rejection Rate (FRR)

A statistic used to measure biometric performance when operating in the verification task. The percentage of times the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. Example: John claims to be John, but the system incorrectly denies the claim. *See also false non-match rate, type I error.*

Feature(s)

Distinctive mathematical characteristic(s) derived from a biometric sample; used to generate a reference. *See also extraction, template.*

Feature Extraction

See extraction.

FERET - FacE REcognition Technology program

A face recognition development and evaluation program sponsored by the U.S. Government from 1993 through 1997. For more information visit http://www.frvt.org/FERET/default.htm. *See also FRGC, FRVT.*

Fingerprint Recognition

A biometric modality that uses the physical structure of an individual's fingerprint for recognition purposes. Important features used in most fingerprint recognition systems are minutiae points that include bifurcations and ridge endings. *See also bifurcation, core point, delta point, minutia(e) point.*

FpVTE - Fingerprint Vendor Technology Evaluation (2003)

An independently administered technology evaluation of commercial fingerprint matching algorithms. For more information visit http://fpvte.nist.gov/.

FRGC - Face Recognition Grand Challenge

A face recognition development program sponsored by the U.S. Government from 2003-2005. For more information visit http://www.frvt.org/FRGC/. *See also FERET, FRVT.*

Friction Ridge

The ridges present on the skin of the fingers and toes, and on the palms and soles of the feet, which make contact with an incident surface under normal touch. On the fingers, the distinctive patterns formed by the friction ridges that make up the fingerprints. *See also minutia(e) point.*

FRVT - Face Recognition Vendor Test

A series of large-scale independent technology evaluations of face recognition systems. The evaluations have occurred in 2000, 2002, and 2005. For more information visit http://www.frvt.org/FRVT2005/default.aspx. *See also FRGC, FERET.*

Gallery

The biometric system's database, or set of known individuals, for a specific implementation or evaluation experiment. *See also database, probe.*

Gait

An individual's manner of walking. This behavioral characteristic is in the research and development stage of automation.

Hamming Distance

The number of non-corresponding digits in a string of binary digits; used to measure dissimilarity. Hamming distances are used in many Daugman iris recognition algorithms. *See also difference score, similarity score.*

Hand Geometry Recognition

A biometric modality that uses the physical structure of an individual's hand for recognition purposes.

ICE - Iris Challenge Evaluation

A large-scale development and independent technology evaluation activity for iris recognition systems sponsored by the U.S. Government in 2005. .For more information visit http://iris.nist.gov/ICE/.

Identification

A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity. *See also closed-set identification, open-set identification, verification, watchlist.*

Identification Rate

The rate at which an individual in a database is correctly identified.

Impostor

A person who submits a biometric sample in either an intentional or inadvertent attempt to claim the identity of another person to a biometric system. *See also attempt.*

INCITS - International Committee for Information Technology Standards

Organization that promotes the effective use of information and communication technology through standardization in a way that balances the interests of all stakeholders and increases the global competitiveness of the member organizations. For more information visit http://www.INCITS.org/. *See also ANSI, ISO, NIST.*

Indifferent User

An individual who knows his/her biometric sample is being collected and does not attempt to help or hinder the collection of the sample. For example, an individual, aware that a camera is being used for face recognition, looks in the general direction of the sensor, neither avoiding nor directly looking at it. *See also* *cooperative user*, *non-cooperative user*, *uncooperative user*.

Infrared

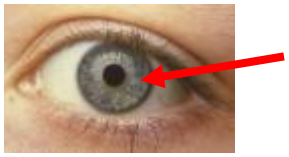
Light that lies outside the human visible spectrum at its red (low frequency) end.

Integrated Automated Fingerprint Identification System (IAFIS)

The FBI's large-scale ten fingerprint (open-set) identification system that is used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provides automated and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and responses. *See also* *AFIS*.

Iris Recognition

A biometric modality that uses an image of the physical structure of an individual's iris for recognition purposes, as illustrated below. The iris muscle is the colored portion of the eye surrounding the pupil.



IrisCode©

A biometric feature format used in the Daugman iris recognition system.

ISO - International Organization for Standardization

A non-governmental network of the national standards institutes from 151 countries. The ISO acts as a bridging organization in which a consensus can be reached on solutions that meet both the requirements of business and the broader needs of society, such as the needs of stakeholder groups like consumers and users. For more information visit http://www.iso.org. *See also* *ANSI*, *INCITS*, *NIST*.

Keystroke Dynamics

A biometric modality that uses the cadence of an individual's typing pattern for recognition.

Latent Fingerprint

A fingerprint "image" left on a surface that was touched by an individual. The transferred impression is left by the surface contact with the friction ridges, usually caused by the oily residues produced by the sweat glands in the finger. *See also friction ridge.*

Live Capture

Typically refers to a fingerprint capture device that electronically captures fingerprint images using a sensor (rather than scanning ink-based fingerprint images on a card or lifting a latent fingerprint from a surface). *See also sensor.*

Liveness Detection

A technique used to ensure that the biometric sample submitted is from an end user. A liveness detection method can help protect the system against some types of spoofing attacks. *See also challenge response, mimic, spoofing.*

Loop

A fingerprint pattern in which the friction ridges enter from either side, curve sharply and pass out near the same side they entered as illustrated below. This pattern will contain one core and one delta. *See also arch, core point, delta point, friction ridge, whorl.*

Match

A decision that a biometric sample and a stored template comes from the same human source, based on their high level of similarity (difference or hamming distance). *See also false match rate, false non-match rate.*

Matching

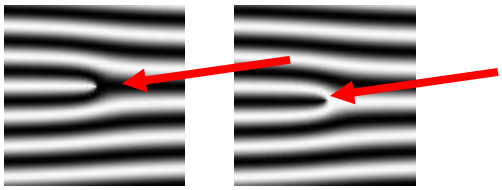
The process of comparing a biometric sample against a previously stored template and scoring the level of similarity (difference or hamming distance). Systems then make decisions based on this score and its relationship (above or below) a predetermined threshold. *See also comparison, difference score, threshold.*

Mimic

The presentation of a live biometric measure in an attempt to fraudulently impersonate someone other than the submitter. *See also challenge response, liveness detection, spoofing.*

Minutia(e) Point

Friction ridge characteristics that are used to individualize a fingerprint image, see illustration below. Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae (as opposed to the images) are compared for recognition purposes. *See also friction ridge, ridge ending.*



Modality

A type or class of biometric system. For example: face recognition, fingerprint recognition, iris recognition, etc.

Model

A representation used to characterize an individual. Behavioral-based biometric systems, because of the inherently dynamic characteristics, use models rather than static templates. *See also template.*

Multimodal Biometric System

A biometric system in which two or more of the modality components (biometric characteristic, sensor type or feature extraction algorithm) occurs in multiple.

Neural Net/Neural Network

A type of algorithm that learns from past experience to make decisions. *See also algorithm.*

NIST - National Institute of Standards and Technology

A non-regulatory federal agency within the U.S. Department of Commerce that develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's measurement and standards work promotes the well-being of the nation and helps improve, among many others things, the nation's homeland security. For more information visit http://www.nist.gov/. *See also ANSI, INCITS, ISO.*

Noise

Unwanted components in a signal that degrade the quality of data or interfere with the desired signals processed by a system.

Non-cooperative User

An individual who is not aware that his/her biometric sample is being collected. Example: A traveler passing through a security line at an airport is unaware that a camera is capturing his/her face image. *See also cooperative user, indifferent user, uncooperative user.*

One-to-many

A phrase used in the biometrics community to describe a system that compares one reference to many enrolled references to make a decision. The phrase typically refers to the identification or watchlist tasks.

One-to-one

A phrase used in the biometrics community to describe a system that compares one reference to one enrolled reference to make a decision. The phrase typically refers to the verification task (though not all verification tasks are truly one-to-one) and the identification task can be accomplished by a series of one-to-one comparisons.

Open-set Identification

Biometric task that more closely follows operational biometric system conditions to 1) determine if someone is in a database and 2) find the record of the individual in the database. This is sometimes referred to as the "watchlist" task to differentiate it from the more commonly referenced closed-set identification. *See also closed-set identification, identification.*

Operational Evaluation

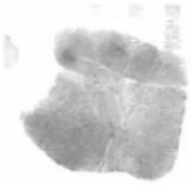
One of the three types of performance evaluations. The primary goal of an operational evaluation is to determine the workflow impact seen by the addition of a biometric system. *See also technology evaluation, scenario evaluation.*

Overt

Biometric sample collection where end users know they are being collected and at what location. An example of an overt environment is the US-VISIT program where non-U.S. citizens entering the United States submit their fingerprint data. *See also covert.*

Palm Print Recognition

A biometric modality that uses the physical structure of an individual's palm print for recognition purposes, as illustrated below.



Performance

A catch-all phrase for describing a measurement of the characteristics, such as accuracy or speed, of a biometric

algorithm or system. *See also accuracy, crossover error rate, cumulative match characteristics, d-prime, detection error trade-off, equal error rate, false accept rate, false alarm rate, false match rate, false reject rate, identification rate, operational evaluation, receiver operating characteristics, scenario evaluation, technology evaluation, true accept rate, true reject rate, verification rate.*

PIN - Personal Identification Number

A security method used to show "what you know." Depending on the system, a PIN could be used to either claim or verify a claimed identity.

Pixel

A picture element. This is the smallest element of a display that can be assigned a color value. *See also pixels per inch (PPI), resolution.*

Pixels Per Inch (PPI)

A measure of the resolution of a digital image. The higher the PPI, the more information is included in the image, and the larger the file size. *See also pixel, resolution.*

Population

The set of potential end users for an application.

Probe

The biometric sample that is submitted to the biometric system to compare against one or more references in the gallery. *See also gallery.*

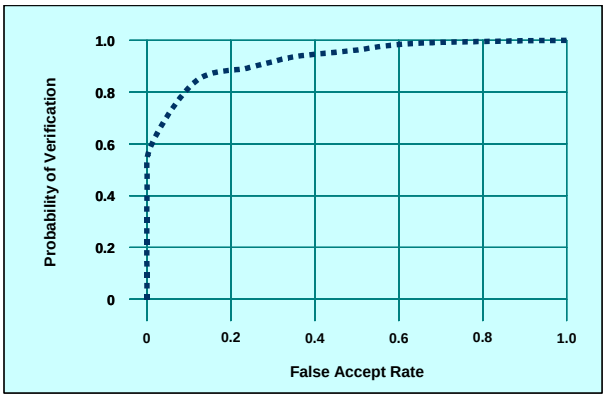
Radio Frequency Identification (RFID)

Technology that uses low-powered radio transmitters to read data stored in a transponder (tag). RFID tags can be used to track assets, manage inventory, authorize payments, and serve as electronic keys. RFID is not a biometric.

Receiver Operating Characteristics (ROC)

A method of showing measured accuracy performance of a biometric system. A verification ROC compares false accept rate vs. verification rate. An open-set identification (watchlist) ROC compares false alarm rates vs. detection and identification rate.

Receiver Operating Characteristic



Recognition

A generic term used in the description of biometric systems (e.g. face recognition or iris recognition) relating to their fundamental function. The term "recognition" does not inherently imply the verification, closed-set identification or open-set identification (watchlist).

Record

The template and other information about the end user (e.g. name, access permissions).

Reference

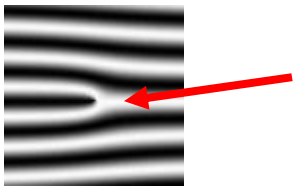
The biometric data stored for an individual for use in future recognition. A reference can be one or more templates, models or raw images. *See also template.*

Resolution

The number of pixels per unit distance in the image. Describes the sharpness and clarity of an image. *See also pixel, pixels per inch (PPI).*

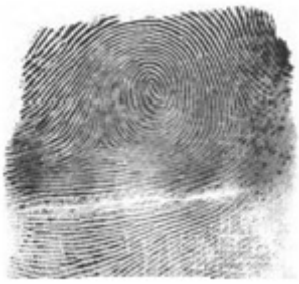
Ridge Ending

A minutiae point at the ending of a friction ridge, as illustrated below. *See also bifurcation, friction ridge.*



Rolled Fingerprints

An image that includes fingerprint data from nail to nail, obtained by "rolling" the finger across a sensor, as illustrated below.



Scenario Evaluation

One of the three types of performance evaluations. The primary goal of a scenario evaluation is to measure performance of a biometric system operating in a specific application. *See also technology evaluation, operational evaluation.*

Segmentation

The process of parsing the biometric signal of interest from the entire acquired data system. For example, finding individual finger images from a slap impression, as illustrated below.

Sensor

Hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.

Sensor Aging

The gradual degradation in performance of a sensor over time.

Signature Dynamics

A behavioral biometric modality that analyzes dynamic characteristics of an individual's signature, such as shape of signature, speed of signing, pen pressure when signing, and pen-in-air movements, for recognition.

Similarity Score

A value returned by a biometric algorithm that indicates the degree of similarity or correlation between a biometric sample and a reference. *See also difference score, hamming distance.*

Skimming

The act of obtaining data from an unknowing end user who is not willingly submitting the sample at that time. An example could be secretly reading data while in close proximity to a user on a bus. *See also eavesdropping.*

Slap Fingerprint

Fingerprints taken by simultaneously pressing the four fingers of one hand onto a scanner or a fingerprint card, as illustrated below. Slaps are known as four finger simultaneous plain impressions.

Speaker Recognition

A biometric modality that uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes. Sometimes referred to as "voice recognition." "Speech recognition" recognizes the words being said, and is not a biometric technology. *See also speech recognition, voice recognition.*

Speaker Recognition Evaluations

An ongoing series of evaluations of speaker recognition systems. For more information, visit http://www.nist.gov/speech/tests/spk/index.htm.

Speech Recognition

A technology that enables a machine to recognize spoken words. Speech recognition is not a biometric technology. *See also speaker recognition, voice recognition.*

Spoofing

The ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone that is in the database. *See also liveness detection, mimic.*

Submission

The process whereby an end user provides a biometric sample to a biometric system. *See also capture.*

Technology Evaluation

One of the three types of performance evaluations. The primary goal of a technology evaluation is to measure performance of biometric systems, typically only the recognition algorithm component, in general tasks. *See also operational evaluation, scenario evaluation.*

Template

A digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. *See also extraction, feature, model.*

Threat

An intentional or unintentional potential event that could compromise the security and integrity of the system. *See also vulnerability.*

Threshold

A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. The acceptance or rejection of biometric data is dependent on the match score

falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application. *See also comparison, match, matching.*

Throughput Rate

The number of biometric transactions that a biometric system processes within a stated time interval.

Token

A physical object that indicates the identity of its owner. For example, a smart card.

True Accept Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) verifies a true claim of identity. For example, Frank claims to be Frank and the system verifies the claim.

True Reject Rate

A statistic used to measure biometric performance when operating in the verification task. The percentage of times a system (correctly) rejects a false claim of identity. For example, Frank claims to be John and the system rejects the claim.

Type I Error

An error that occurs in a statistical test when a true claim is (incorrectly) rejected. For example, John claims to be John, but the system incorrectly denies the claim. *See also false reject rate (FRR).*

Type II Error

An error that occurs in a statistical test when a false claim is (incorrectly) not rejected. For example: Frank claims to be John and the system verifies the claim. *See also false accept rate (FAR).*

Uncooperative User

An individual who actively tries to deny the capture of his/her biometric data. Example: A detainee mutilates his/her finger upon capture to prevent the recognition of his/her identity via fingerprint. *See also cooperative user, indifferent user, non-cooperative user.*

User

A person, such as an administrator, who interacts with or controls end users' interactions with a biometric system. *See also cooperative user, end user, indifferent user, non-cooperative user, uncooperative user.*

US-VISIT - U.S. Visitor and Immigrant Status Indicator Technology

A continuum of security measures that begins overseas, at the Department of State's visa issuing posts, and continues through arrival and departure from the United States of America. Using biometric, such as digital, inkless fingerscans and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the U.S. border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the U.S. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a know security risk (including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry and exit procedures address the U.S. critical need for tighter security and ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country.

Verification

A task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. *See also identification, watchlist.*

Verification Rate

A statistic used to measure biometric performance when operating in the verification task. The rate at which legitimate end-users are correctly verified.

Voice Recognition

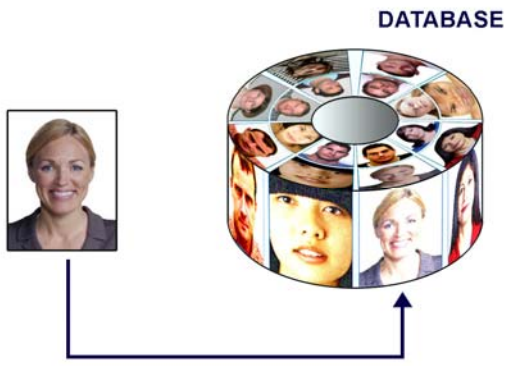
See speaker recognition.

Vulnerability

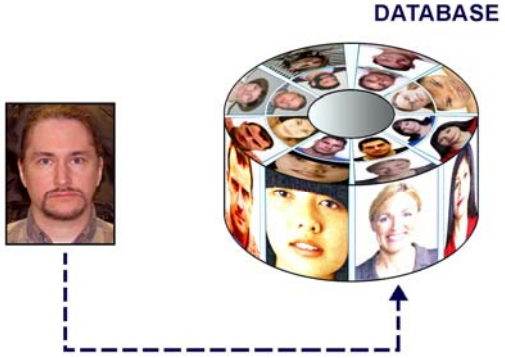
The potential for the function of a biometric system to be compromised by intent (fraudulent activity); design flaw (including usage error); accident; hardware failure; or external environmental condition. *See also threat.*

Watchlist

A term sometimes referred to as open-set identification that describes one of the three tasks that biometric systems perform. Answers the questions: Is this person in the database? If so, who are they? The biometric system determines if the individual's biometric template matches a biometric template of someone on the watchlist, as illustrated below. The individual does not make an identity claim, and in some cases does not personally interact with the system whatsoever. *See also closed-set identification, identification, open-set identification, verification.*



(This individual is in the watchlist)



(This individual is not in the watchlist)

Wavelet Scalar Quantization (WSQ)

An FBI-specified compression standard algorithm that is used for the exchange of fingerprints within the criminal justice community. It is used to reduce the data size of images.

Whorl

A fingerprint pattern in which the ridges are circular or nearly circular, as illustrated below. The pattern will contain 2 or more deltas. *See also arch, delta point, loop, minutia(e) point.*

National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Introduction

The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago.

One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Since the beginning of civilization, humans have used faces to identify known (familiar) and unknown (unfamiliar) individuals. This simple task became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into- once small communities. The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as speaker and gait recognition. Individuals use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis.

Other characteristics have also been used throughout the history of civilization as a more formal means of recognition. Some examples are:

- In a cave estimated to be at least 31,000 years old, the walls are adorned with paintings believed to be created by prehistoric men who lived there. Surrounding these paintings are numerous handprints that are felt to "have…acted as an un-forgeable signature" of its originator. [1]
- There is also evidence that fingerprints were used as a person's mark as early as 500 B.C. "Babylonian business transactions are recorded in clay tablets that include fingerprints." [2]
- Joao de Barros, a Spanish explorer and writer, wrote that early Chinese merchants used fingerprints to settle business transactions. Chinese parents also used fingerprints and footprints to differentiate children from one another. [3]
- In early Egyptian history, traders were identified by their physical descriptors to differentiate between

trusted traders of known reputation and previous successful transactions, and those new to the market. [3]

By the mid-1800s, with the rapid growth of cities due to the industrial revolution and more productive farming, there was a formally recognized need to identify people. Merchants and authorities were faced with increasingly larger and more mobile populations and could no longer rely solely on their own experiences and local knowledge. Influenced by the writings of Jeremy Betham and other Utilitarian thinkers, the courts of this period began to codify concepts of justice that endure with us to this day. Most notably, justice systems sought to treat first time offenders more leniently and repeat offenders more harshly. This created a need for a formal system that recorded offenses along with measured identity traits of the offender. The first of two approaches was the Bertillon system of measuring various body dimensions, which originated in France. These measurements were written on cards that could be sorted by height, arm length or any other parameter. This field was called anthropometrics. The other approach was the formal use of fingerprints by police departments. This process emerged in South America, Asia, and Europe. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records as Bertillon's method did but that was based on a more individualized metric – fingerprint patterns and ridges. The first such robust system for indexing fingerprints was developed in India by Azizul Haque for Edward Henry, Inspector General of Police, Bengal, India. This system, called the Henry System, and variations on it are still in use for classifying fingerprints. [4]

True biometric systems began to emerge in the latter half of the twentieth century, coinciding with the emergence of computer systems. The nascent field experienced an explosion of activity in the 1990s and began to surface in everyday applications in the early 2000s.

Condensed Timeline of Biometrics History

KEY	Iris
Biometrics	Palm
Face	Signature
Fingerprint	Speech
Hand Geometry	Vascular

Year	Description
1858	First systematic capture of hand images for identification purposes is recorded
1870	Bertillon develops anthropometrics to identify individuals
1892	Galton develops a classification system for fingerprints
1894	The Tragedy of Pudd'nhead Wilson is published
1896	Henry develops a fingerprint classification system
1903	NY State Prisons begins using fingerprints
1903	Bertillon System collapses
1936	Concept of using the iris pattern for identification is proposed
1960s	Face recognition becomes semi-automated
1960	First model of acoustic speech production is created
1963	Hughes research paper on fingerprint automation published
1965	Automated signature recognition research begins
1969	FBI pushes to make fingerprint recognition an automated process
1970s	Face Recognition takes another step towards automation
1970	Behavioral components of speech are first modeled
1974	First commercial hand geometry systems become available
1975	FBI funds development of sensors and minutiae extracting technology

Biometrics History

Year	Description
1976	First prototype system for speaker recognition is developed
1977	Patent is awarded for acquisition of dynamic signature information
1980s	NIST Speech Group is established
1985	Concept that no two irides are alike is proposed
1985	Patent for hand identification is awarded
1986	Exchange of fingerprint minutiae data standard is published
1987	Patent stating that the iris can be used for identification is awarded
1988	First semi-automated facial recognition system is deployed
1988	Eigenface technique is developed for face recognition
1991	Face detection is pioneered, making real time face recognition possible
1992	Biometric Consortium is established within US Government
1993	Development of an iris prototype unit begins
1993	FacE REcognition Technology (FERET) program is initiated
1994	First iris recognition algorithm is patented
1994	Integrated Automated Fingerprint Identification System (IAFIS) competition is held
1994	Palm System is benchmarked
1994	INSPASS is implemented
1995	Iris prototype becomes available as a commercial product
1996	Hand geometry is implemented at the Olympic Games
1996	NIST begins hosting annual speaker recognition evaluations
1997	First commercial, generic biometric interoperability standard is published
1998	FBI launches CODIS (DNA forensic database)
1999	Study on the compatibility of biometrics and machine readable travel documents is launched
1999	FBI's IAFIS major components become operational

Year	Description
2000	First Face Recognition Vendor Test (FRVT 2000) is held
2000	First research paper describing the use of vascular patterns for recognition is published
2000	West Virginia University biometrics degree program is established
2001	Face recognition is used at the Super Bowl in Tampa, Florida
2002	ISO/IEC standards subcommittee on biometrics is established
2002	M1 Technical Committee on Biometrics is formed
2002	Palm Print Staff Paper is submitted to Identification Services Committee
2003	Formal US Government coordination of biometric activities begins
2003	ICAO adopts blueprint to integrate biometrics into machine readable travel documents
2003	European Biometrics Forum is established
2004	US-VISIT program becomes operational
2004	DOD implements ABIS
2004	Presidential directive calls for mandatory government-wide personal identification card for all federal employees and contractors
2004	First statewide automated palm print database is deployed in the US
2004	Face Recognition Grand Challenge begins
2005	US patent on iris recognition concept expires
2005	Iris on the Move™ is announced at Biometrics Consortium Conference

1858 - First systematic capture of hand images for identification purposes is recorded

Sir William Herschel, working for the Civil Service of India, recorded a handprint on the back of a contract for each worker to distinguish employees from others who might claim to be employees when payday arrived. This was the first recorded systematic capture of hand and finger images that were uniformly taken for identification purposes.

Peter Komarinski, Automated Fingerprint Identification Systems (need publisher info) 29.

1870 - Bertillon develops anthropometrics to identify individuals

Alphonse Bertillon developed "Bertillonage" or anthropometrics, a method of identifying individuals based on detailed records of their body measurements, physical descriptions and photographs. Repeat criminal offenders often provided different aliases when arrested. Bertillon noted that although they could change their names, they could not change certain elements of their bodies. Police authorities throughout the world used his system, until its use quickly faded when it was discovered that some people shared the same measurements. The Bertillon documents (in French) are available at http://www.biometricscatalog.org/documents/Bertillon%20Documents%20%28French%29-1.pdf.

1892 - Galton develops a classification system for fingerprints

Sir Francis Galton wrote a detailed study of fingerprints in which he presented a new classification system using prints from all ten fingers. The characteristics (minutiae) that Galton used to identify individuals are still used today. These details are often referred to as Galton's details.

"Sir Francis Galton," Galton.org <http://galton.org/>.

1894 - The Tragedy of Pudd'nhead Wilson is published

In The Tragedy of Pudd'nhead Wilson, author Mark Twain mentions the use of fingerprints for identification. In the story, a man on trial calls on the comparison of his fingerprints to those left at the crime scene to prove his innocence.

1896 - Henry develops a fingerprint classification system

Sir Edward Henry, Inspector General of the Bengal Police, was in search of a method of identification to implement concurrently or to replace anthropometrics. Henry consulted Sir Francis Galton regarding fingerprinting as a method of identifying criminals. Once the fingerprinting system was implemented, one of Henry's workers, Azizul Haque, developed a method of classifying and

storing the information so that searching could be performed easily and efficiently. Sir Henry later established the first British fingerprint files in London. The Henry Classification System, as it came to be known, was the precursor to the classification system used for many years by the Federal Bureau of Investigation (FBI) and other criminal justice organizations that perform tenprint fingerprint searches.

> "Fingerprint Centenary: Press Pack - Sir Edward Henry (1850-1931)," Metropolitan Police <http://www.met.police.uk/so/100years/henry.htm>.

1903 - NY State Prisons begin using fingerprints

"The New York Civil Service Commission established the practice of fingerprinting applicants to pre-vent them from having better qualified persons take their tests for them." This practice was adopted by the New York state prison system where fingerprints were used "for the identification of criminals in 1903. In 1904 the fingerprint system accelerated when the United States Penitentiary at Leavenworth, Kansas, and the St. Louis, Missouri, Police Department both established fingerprint bureaus. During the first quarter of the 20th century, more and more local police identification bureaus established fingerprint systems. The growing need and demand by police officials for a national repository and clearinghouse for fingerprint records led to an Act of Congress on July 1, 1921, establishing the Identification Division of the FBI."

> "Homeland Security: Fingerprint Identification Systems" 27 April 2005, GlobalSecurity.org <http://www.globalsecurity.org/security/systems/fingerprint.htm>.

1903 - Bertillon System collapses

Two men, determined later to be identical twins, were sentenced to the US Penitentiary at Leavenworth, KS, and were found to have nearly the same measurements using the Bertillon system. Although the basis of this story has been subsequently challenged, the story was used to argue that Bertillon measurements were inadequate to differentiate between these two individuals.

> "The History of Fingerprints" 26 December 2005 <http://onin.com/fp/fphistory.html>.

1936 - Concept of using the iris pattern for identification is proposed

Ophthalmologist Frank Burch proposed the concept of using iris patterns as a method to recognize an individual.

> "Individual Biometrics: Iris Scan" 5 July 05, National Center for State Courts 6 July 06 <http://ctl.ncsc.dni.us/biomet%20web/BMIris.html>.

1960s - Face recognition becomes semi-automated

The first semi-automatic face recognition system was developed by Woodrow W. Bledsoe under contract to the US Government. This system required the administrator to locate features such as eyes, ears, nose and mouth on the photographs. This system relied solely on the ability to extract useable feature points. It calculated distances and ratios to a common reference point that was compared to the reference data.

> "In Memoriam Woodrow Wilson Bledsoe," The University of Texas at Austin, Department of Computer Science <http://www.cs.utexas.edu/users/boyer/bledsoe-memorial-resolution.pdf>.

1960 - First model of acoustic speech production is created

A Swedish Professor, Gunnar Fant, published a model describing the physiological components of acoustic speech production. His findings were based on the analysis of x-rays of individuals making specified phonic sounds. These findings were used to better understand the biological components of speech, a concept crucial to speaker recognition.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

1963 - Hughes research paper on fingerprint automation is published

> M. Trauring, "Automatic comparison of finger ridge patterns," Report No. 190, Hughes Research Laboratories, March 1961, Rev. April 1963.

1965 - Automated signature recognition research begins

North American Aviation developed the first signature recognition system in 1965.

> A. J. Mauceri, "Feasibility Studies of Personal Identification by Signature Verification", Report no. SID 65 24 RADC TR 65 33, Space and Information System Division, North American Aviation Co., Anaheim, USA, 1965.

1969 - FBI pushes to make fingerprint recognition an automated process

In 1969, the Federal Bureau of Investigation (FBI) began its push to develop a system to automate its fingerprint identification process, which was quickly becoming overwhelming and required many man-hours. The FBI contracted the National Institute of Standards and Technology (NIST) to study the process of automating fingerprint identification. NIST identified two key challenges: (1) scanning fingerprint cards and identifying minutiae and (2) comparing and matching lists of minutiae.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

1970s - Face Recognition takes another step towards automation

Goldstein, Harmon, and Lesk used 21 specific subjective markers such as hair color and lip thickness to automate face recognition. The problem with both of these early solutions was that the measurements and locations were manually computed.

> A. J. Goldstein, L. D. Harmon, and A. B. Lesk, "Identification of Human Faces," Proc. IEEE, Vol. 59, No. 5, May 1971, 748-760.

1970 - Behavioral components of speech are first modeled

The original model of acoustic speech production, developed in 1960, was expanded upon by Dr. Joseph Perkell, who used motion x-rays and included the tongue and jaw. The model provided a more detailed understanding of the complex behavioral and biological components of speech.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

1974 - First commercial hand geometry systems become available

The first commercial hand geometry recognition systems became available in the early 1970s, arguably the first commercially available biometric device after the early deployments of fingerprinting in the late 1960s. These systems were implemented for three main purposes: physical access control; time and attendance; and personal identification.

> IR Recognition Systems <http://recogsys.com/index.shtml>.

1975 - FBI funds development of sensors and minutiae extracting technology

The FBI funded the development of scanners and minutiae extracting technology, which led to the development of a prototype reader. At this point, only the minutiae were stored because of the high cost of digital storage. These early readers used capacitive techniques to collect the fingerprint characteristics. Over the next decades, NIST focused on and led developments in automatic methods of digitizing inked fingerprints and the effects of image compression on image quality, classification, extraction of minutiae, and matching. The work at NIST led to the development of the M40 algorithm, the first operational matching algorithm used at the FBI. Used to narrow the human search, this algorithm produced a significantly smaller set of images that were then provided to trained and specialized human technicians for evaluation. Developments continued to improve the available fingerprint technology.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).
>
> Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).
>
> James Wayman, et al, Biometric Systems Technology, Design and Performance Evaluation (London: Springer, 2005).

1976 - First prototype system for speaker recognition is developed

Texas Instruments developed a prototype speaker recognition system that was tested by the US Air Force and The MITRE Corporation.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).
>
> W. Haberman and A. Fejfar, "Automatic ID of Personnel through Speaker and Signature Verification – System Description and Testing," May 1976 Carnahan Conference on Crime Countermeasures, University of Kentucky.

1977 - Patent is awarded for acquisition of dynamic signature information

Veripen, Inc. was awarded a patent for a "Personal identification apparatus" that was able to acquire dynamic pressure information. This device allowed the digital capture of the dynamic characteristics of an individual's signature characteristics. The development of this technology led to the testing of automatic handwriting verification (performed by The MITRE Corporation) for the Electronic Systems Division of the United States Air Force.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins. Biometrics (New York: McGraw Hill Osborne, 2003).

1980s - NIST Speech Group is established

The National Institute of Standards and Technology (NIST) developed the NIST Speech Group to study and promote the use of speech processing techniques. Since 1996, under funding from the National Security Agency, the NIST Speech Group has hosted yearly evaluations — the NIST Speaker Recognition Evaluation Workshop — to foster the continued advancement of the speaker recognition community.

> "NIST Speaker Recognition Evaluations" 25 April 2005, NIST Speech Group, 23 June 2005 <http://www.nist.gov/speech/tests/spk/index.htm>.

1985 - Concept that no two irides are alike is proposed

Drs. Leonard Flom and Aran Safir, ophthalmologists, proposed the concept that no two irides are alike.

> "Individual Biometrics: Iris Scan" 5 July 05, National Center for State Courts 6 July 06 <http://ctl.ncsc.dni.us/biomet%20web/BMIris.html>.

1985 - Patent for hand identification is awarded

The commercialization of hand geometry dates to the early 1970s with one of the first deployments at the University of Georgia in 1974. The US Army began testing hand geometry for use in banking in about 1984. These deployments predate the concept of using the geometry of a hand for identification as patented by David Sidlauskas.

> United States Patent and Trademark Office. "Patent 4,736,203: 3D hand profile identification apparatus." 5 April 1988 <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=4,736,203.WKU.&OS=PN/4,736,203&RS=PN/4,736,203>.

1986 - Exchange of fingerprint minutiae data standard is published

The National Bureau of Standards (NBS) — now the National Institutes of Standards and Technology (NIST) — published, in collaboration with ANSI, a standard for the exchange of fingerprint minutiae data (ANSI/NBS-ICST 1-1986). This was the first version of the current fingerprint interchange standards used by law enforcement agencies around the world today. More information is available at

http://ai.eller.arizona.edu/COPLINK/publications/develop/develop.html.

> K. Lynch and F. Rodgers, . "Development of Integrated Criminal Justice Expert System Applications."

1986 - Patent is awarded stating that the iris can be used for identification

Drs. Leonard Flom and Aran Safir were awarded a patent for their concept that the iris could be used for identification. Dr. Flom

approached Dr. John Daugman to develop an algorithm to automate identification of the human iris.

> "Historical Timeline," Iridian Technologies <http://www.iridiantech.com/about.php?page=4>.

1988 - First semi-automated facial recognition system is deployed

In 1988, the Lakewood Division of the Los Angeles County Sheriff's Department began using composite drawings (or video images) of a suspect to conduct a database search of digitized mugshots.

> Jarvis, Angela. "Facial Recognition Systems – Are Privacy Rights of Citizens Being Eroded Wholesale?", Forensic-Evidence.com <http://www.forensic-evidence.com/site/ID/facialrecog.html>.

1988 - Eigenface technique is developed for face recognition

Kirby and Sirovich applied principle component analysis, a standard linear algebra technique, to the face recognition problem. This was a milestone because it showed that less than one hundred values were required to approximate a suitably aligned and normalized face image.

> L. Sirovich and M. Kirby. "A Low-Dimensional Procedure for the Characterization of Human Faces," J. Optical Soc. Am. A, Vol. 4, No.3, 1987: 519-524.

1991 - Face detection is pioneered, making real time face recognition possible

Turk and Pentland discovered that while using the eigenfaces techniques, the residual error could be used to detect faces in images. The result of this discovery meant that reliable real time automated face recognition was possible. They found that this was somewhat constrained by environmental factors, but the discovery caused a large spark of interest in face recognition development.

> M. A. Turk and A. P. Pentland. "Face Recognition Using Eigenfaces," Proc. IEEE, 1991: 586-591.

1992 - Biometric Consortium is established within US Government

The National Security Agency initiated the formation of the Biometric Consortium and held its first meeting in October of 1992. The Consortium was chartered in 1995 by the Security Policy Board, which was abolished in 2001.

Participation in the Consortium was originally limited to government agencies; members of private industry and academia were limited to attending in an observer capacity. The Consortium soon expanded its membership to include these communities and developed numerous working groups to initiate and/or expand efforts in testing, standards development, interoperability, and government cooperation. With the explosion of biometric activities in the early 2000s, the activities of these working groups were integrated into other organizations (such as INCITS, ISO, and the NSTC Subcommittee on Biometrics) in order to expand and accelerate their activities and impacts. The Consortium itself remains active as a key liaison and discussion forum between government, industry, and academic communities.

> "Background of the US Government's Biometric Consortium, " The Biometrics Consortium <http://www.biometrics.org/REPORTS/CTST96/>.

1993 - Development of an iris prototype unit begins

The Defense Nuclear Agency began work with IriScan, Inc. to test and deliver a prototype iris recognition unit.

> "Historical Timeline," Iridian Technologies <http://www.iridiantech.com/about.php?page=4>.

1993 - FacE REcognition Technology (FERET) program is initiated

The FacE REcogntion Technology (FERET) Evaluation was sponsored from 1993-1997 by the Defense Advanced Research Products Agency (DARPA) and the DoD Counterdrug Technology Development Program Office in an effort to encourage the development of face recognition algorithms and technology. This evaluation assessed the prototypes of face recognition systems

and propelled face recognition from its infancy to a market of commercial products. More information about FERET can be found at http://www.frvt.org/FERET/default.htm.

> P. J. Phillips, H. Moon, S. A. Rizvi and P. J. Rauss, "The FERET Evaluation Methodology for Face-Recognition Algorithms," IEEE Transactions on PAMI, Vol. 22, No. 10, 2000: 1090-1104.

1994 - First iris recognition algorithm is patented

Dr. John Daugman was awarded a patent for his iris recognition algorithms. Owned by Iridian Technologies, the successor to IriScan, Inc. — this patent is the cornerstone of most commercial iris recognition products to date.

> "Historical Timeline," Iridian Technologies <http://www.iridiantech.com/about.php?page=4>.

1994 - Integrated Automated Fingerprint Identification System (IAFIS) competition is held

The next stage in fingerprint automation occurred at the end of the Integrated Automated Fingerprint Identification System (IAFIS) competition. The competition identified and investigated three major challenges: (1) digital fingerprint acquisition, (2) local ridge characteristic extraction, and (3) ridge characteristic pattern matching. The demonstrated model systems were evaluated based on specific performance requirements. Lockheed Martin was selected to build the FBI's IAFIS.

> Maltoni, Davide, Maio, Jain, and Prabhakar, Handbook of Fingerprint Recognition (Springer: New York, 2005).

1994 - Palm System is benchmarked

The first known Automated Fingerprint Identification Systems (AFIS) system built to support palm prints is believed to have been built by a Hungarian company known as RECOWARE Ltd. In late 1994, latent experts from the United States benchmarked this palm system, RECOderm™, in Hungary and invited RECOWARE Ltd. to the 1995 International Association for Identification (IAI) conference in Costa Mesa, California. The palm and fingerprint

1992 - Biometric Consortium is established within US Government

The National Security Agency initiated the formation of the Biometric Consortium and held its first meeting in October of 1992. The Consortium was chartered in 1995 by the Security Policy Board, which was abolished in 2001.

Participation in the Consortium was originally limited to government agencies; members of private industry and academia were limited to attending in an observer capacity. The Consortium soon expanded its membership to include these communities and developed numerous working groups to initiate and/or expand efforts in testing, standards development, interoperability, and government cooperation. With the explosion of biometric activities in the early 2000s, the activities of these working groups were integrated into other organizations (such as INCITS, ISO, and the NSTC Subcommittee on Biometrics) in order to expand and accelerate their activities and impacts. The Consortium itself remains active as a key liaison and discussion forum between government, industry, and academic communities.

> "Background of the US Government's Biometric Consortium, " The Biometrics Consortium <http://www.biometrics.org/REPORTS/CTST96/>.

1993 - Development of an iris prototype unit begins

The Defense Nuclear Agency began work with IriScan, Inc. to test and deliver a prototype iris recognition unit.

> "Historical Timeline," Iridian Technologies <http://www.iridiantech.com/about.php?page=4>.

1993 - FacE REcognition Technology (FERET) program is initiated

The FacE REcogntion Technology (FERET) Evaluation was sponsored from 1993-1997 by the Defense Advanced Research Products Agency (DARPA) and the DoD Counterdrug Technology Development Program Office in an effort to encourage the development of face recognition algorithms and technology. This evaluation assessed the prototypes of face recognition systems

1996 - NIST begins hosting annual speaker recognition evaluations

Under funding from the National Security Agency, the National Institute of Standards and Technology (NIST) Speech Group began hosting yearly evaluations in 1996. The NIST Speaker Recognition Evaluation Workshop aims to foster the continued advancement of the speaker recognition community.

> "NIST Speaker Recognition Evaluations" 25 April 2005, NIST Speech Group, 23 June 2005 <http://www.nist.gov/speech/tests/spk/index.htm>.

1997 - First commercial, generic biometric interoperability standard is published

Sponsored by NSA, the Human Authentication API (HA-API) was published as the first commercial, generic biometric interoperability standard and focused on easing integration of and allowing for interchangeability and vendor independence. It was a breakthrough in biometric vendors working together to advance the industry through standardization and was the precursor to subsequent biometric standardization activities. Further information is available at http://www.biometrics.org/html/standards.html.

1998 - FBI launches CODIS (DNA forensic database)

The FBI launched Combined DNA Index System (CODIS) to digitally store, search, and retrieve DNA markers for forensic law enforcement purposes. Sequencing is a laboratory process taking between 40 minutes and several hours. More information on DNA identification can be found at the following:

> http://www.fbi.gov/hq/lab/codis/index1.htm
>
> http://www.cstl.nist.gov/div831/
>
> http://www.afip.org/Departments/oafme/dna/

1999 - Study on the compatibility of biometrics and machine readable travel documents is launched

The International Civil Aviation Organization's (ICAO) Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) initiated a study to determine the "compatibility of currently available biometric technologies with the issuance and

inspection processes relevant to MRTDs; and quantifying these compatibilities to determine whether one or more technologies could/should be adopted as the international standard for application in MRTDs."

> "Biometrics - Introduction," Machine Readable Travel Documents 2003 <http://www.icao.int/mrtd/biometrics/intro.cfm>.

1999 - FBI's IAFIS major components become operational

IAFIS, the FBI's large-scale ten-fingerprint (open-set) identification system, became operational. Prior to the development of the standards associated with this system, a fingerprint collected on one system could not be searched against fingerprints on another system. The development of this system addressed the issues associated with communication and information exchange between standalone systems as well as the introduction of a national network for electronic submittal of fingerprints to the FBI. IAFIS is used for criminal history background checks and identification of latent prints discovered at crime scenes. This system provides automated tenprint and latent search capabilities, electronic image storage of fingerprints and facial images, and electronic exchange of fingerprints and search responses.

> Wayman, James, et al. Biometric Systems Technology, Design and Performance Evaluation (London: Springer, 2005).
>
> "Integrated Automated Fingerprint Identification System: What is it?" FBI IAFIS 2 August 2005 <http://www.fbi.gov/hq/cjisd/iafis.htm>.

2000 - First Face Recognition Vendor Test (FRVT 2000) is held

Multiple US Government agencies sponsored the Face Recognition Vendor Test (FRVT) in 2000. FRVT 2000 served as the first open, large-scale technology evaluation of multiple commercially available biometric systems. Additional FRVTs have been held in 2002 and 2006, and the FRVT model has been used to perform evaluations of fingerprint (2003) and iris recognition (2006). FRVT's primary purpose is to evaluate performance on large-scale

databases. More information about each of the FRVTs can be found at http://www.frvt.org.

> "Face Recognition Vendor Test 2000," FRVT.org <http://www.frvt.org/frvt2000/>.

2000 - First research paper describing the use of vascular patterns for recognition is published

This paper describes the technology that was to become the first commercially available vascular pattern recognition system in 2000. The technology uses the subcutaneous blood vessel pattern in the back of the hands to achieve recognition.

> Sang-Kyun Im, Hyung-Man Park, Young-Woo Kim, Sang-Chan Han, Soo-Won Kim and Chul-Hee Kang, "Biometric Identification System by Extracting Hand Vein Patterns," Journal of the Korean Physical Society, Vol. 38, No. 3, March 2001: 268-272.

2000 - West Virginia University biometrics degree program is established

West Virginia University (WVU) and the FBI, in consultation with professional associations such as the International Association for Identification, established a bachelor's degree program in Biometric Systems in 2000. While many universities have long had biometrics-related courses, this is the first biometrics-based degree program. WVU encourages program participants to obtain a dual-degree in Computer Engineering and Biometric Systems as the biometric systems degree is not accredited.

> Duane Blackburn "Biometrics History," Email to West Virginia University, 10 January 2006.

2001 – Face recognition is used at the Super Bowl in Tampa, Florida

A face recognition system was installed at the Super Bowl in January 2001 in Tampa, Florida, in an attempt to identify "wanted" individuals entering the stadium. The demonstration found no "wanted" individuals but managed to misidentify as many as a dozen innocent sports fans. Subsequent media and Congressional inquiries served to introduce both biometrics and its associated privacy concerns into the consciousness of the general public.

2002 - ISO/IEC standards committee on biometrics is established

The International Organization for Standardization (ISO) established the ISO/IEC JTC1 Subcommittee 37 (JTC1/SC37) to support the standardization of generic biometric technologies. The Subcommittee develops standards to promote interoperability and data interchange between applications and systems. More information about JTC1/SC37 can be found at http://www.iso.org/.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

2002 - M1 Technical Committee on Biometrics is formed

The M1 Technical Committee on Biometrics is the US Technical Advisory Group (TAG) to the JTC1/SC37. This technical committee reports to the InterNational Committee on Information Technology Standards (INCITS), an accredited organization of the American National Standards Institute (ANSI), which facilitates the development of standards among accredited organizations. More information about M1 can be found at http://www.ncits.org/tc_home/m1.htm. More information about INCITS can be found at http://www.incits.org/. More information about ANSI can be found at http://www.ansi.org/.

> John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

2002 - Palm Print Staff Paper is submitted to Identification Services Committee

In April 2002, a Staff Paper on palm print technology and Integrated Automated Fingerprint Identification System (IAFIS) palm print capabilities was submitted to the Identification Services (IS) Subcommittee, Criminal Justice Information Services Division (CJIS) Advisory Policy Board (APB). The Joint Working Group called "for strong endorsement of the planning, costing, and development of an integrated latent print capability for palms at the CJIS Division of the FBI." As a result of this endorsement and other changing business needs for law enforcement, the FBI announced the Next Generation IAFIS (NGI)

initiative. A major component of the NGI initiative is development of the requirements for and deployment of an integrated National Palm Print Service.

> NSTC Subcommittee on Biometrics, "Palm Recognition Foundation Document," December 2005.

2003 - Formal US Government coordination of biometric activities begins

The National Science & Technology Council, a US Government cabinet-level council, established a Subcommittee on Biometrics to coordinate biometrics R&D, policy, outreach, and international collaboration. More information can be found at http://www.biometricscatalog.org/NSTCSubcommittee/default.asp.

2003 - ICAO adopts blueprint to integrate biometrics into machine readable travel documents

"On May, 28 2003, The International Civil Aviation Organization (ICAO) adopted a global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs)… Facial recognition was selected as the globally interoperable biometric for machine-assisted identity confirmation with MRTDs."

> "Biometrics - ICAO Recommendation," Machine Readable Travel Documents 2003 <http://www.icao.int/mrtd/biometrics/recommendation.cfm>.

2003 - European Biometrics Forum is established

"The European Biometrics Forum is an independent European organisation supported by the European Commission whose overall vision is to establish the European Union as the World Leader in Biometrics Excellence by addressing barriers to adoption and fragmentation in the marketplace. The forum also acts as the driving force for coordination, support and strengthening of the national bodies."

> "About the EBF," 29 October 2003, European Biometrics Forum (updated 17 January 2006) <http://www.eubiometricforum.com/index.php?option=content&task=view&id=2&Itemid=28>.

2004 - US-VISIT program becomes operational

The United States Visitor and Immigrant Status Indication Technology (US-VISIT) program is the cornerstone of the DHS visa issuance and entry/exit strategy. The US-VISIT program is a continuum of security measures that begins overseas at the Department of State's visa issuing posts, and continues through arrival to and departure from the US. Using biometrics, such as digital inkless fingerprints and digital photographs, the identity of visitors requiring a visa is now matched at each step to ensure that the person crossing the US border is the same person who received the visa. For visa-waiver travelers, the capture of biometrics first occurs at the port of entry to the US. By checking the biometrics of a traveler against its databases, US-VISIT verifies whether the traveler has previously been determined inadmissible, is a known security risk (including having outstanding wants and warrants), or has previously overstayed the terms of a visa. These entry/exit procedures address the US critical need for tighter security and its ongoing commitment to facilitate travel for the millions of legitimate visitors welcomed each year to conduct business, learn, see family, or tour the country.

> "Travel and Transportation: US-VISIT Program," Department of Homeland Security <http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml>.

2004 - DOD implements ABIS

The Automated Biometric Identification System (ABIS) is a Department of Defense (DoD) system implemented to improve the US Government's ability to track and identify national security threats. The associated collection systems include the ability to collect, from enemy combatants, captured insurgents, and other persons of interest, ten rolled fingerprints, up to five mug shots from varying angles, voice samples (utterances), iris images, and an oral swab to collect DNA. More information on the ABIS can be found at http://www.biometrics.dod.mil/default.aspx.

2004 - Presidential directive calls for mandatory government-wide personal identification card for all federal employees and contractors

In 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12) for a mandatory, government-wide

personal identification card that all federal government departments and agencies will issue to their employees and contractors requiring access to Federal facilities and systems. Subsequently, Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) for Federal Employees and Contractors, specifies the technical and operational requirements for the PIV system and card. NIST Special Publication 800-76 (Biometric Data Specification for Personal Identity Verification) is a companion document to FIPS 201 describing how the standard will be acquiring, formatting and storing fingerprint images and templates for collecting and formatting facial images; and specifications for biometric devices used to collect and read fingerprint images. The publication specifies that two fingerprints be stored on the card as minutia templates. Additional information is available at http://csrc.nist.gov/piv-program/index.html.

2004 - First statewide automated palm print databases are deployed in the US

In 2004, Connecticut, Rhode Island and California established statewide palm print databases that allow law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders. Detailed information can be found at:

http://www.necus.com/companies/20/NECSAMCustomerAwardByCalifCenterDigitalGovt.pdf#search='first%20automated%20palm%20system

http://cogt.client.shareholder.com/ReleaseDetail.cfm?ReleaseID=145765

2004 - Face Recognition Grand Challenge begins

The Face Recognition Grand Challenge (FRGC) is a US Government-sponsored challenge problem posed to develop algorithms to improve specific identified areas of interest in face recognition. Participating researchers analyze the provided data, try to solve the problem, and then reconvene to discuss various approaches and their results — an undertaking that is driving technology improvement. Participation in this challenge demonstrates an expansive breadth of knowledge and interest in this biometric modality. More information on the FRGC can be found at http://www.frvt.org/FRGC/.

2005 - US patent for iris recognition concept expires

The broad US patent covering the basic concept of iris recognition expired in 2005, providing marketing opportunities for other companies that have developed their own algorithms for iris recognition. However, the patent on the IrisCodes® implementation of iris recognition developed by Dr. Daugman will not expire until 2011.

2005 - Iris on the Move™ is announced at Biometrics Consortium Conference

At the 2005 Biometrics Consortium conference, Sarnoff Corporation demonstrated Iris on the Move™, a culmination of research and prototype systems sponsored by the Intelligence Technology Innovation Center (ITIC), and previously by the Defense Advanced Research Projects Agency (DARPA). The system enables the collection of iris images from individuals walking through a portal.

> "Iris on the Move™ - A Superior Solution for Biometric Identification," 22 September 2005 (Press Release), Sarnoff Corporation <http://www.sarnoff.com/products_services/government_solutions/homeland_security/iris.asp>.

Document References

[1] Janeen Renaghan, "Etched in Stone," Zoogoer, August 1997, (Smithsonian National Zoological Park, 26 January 2005).

[2] "Dermatoglyphics," Hand Analysis, International Institute of Hand Analysis, 24 January 2005.

[3] Z. McMahon, Biometrics: History, Indiana University, Indiana University Computer Science Department, 24 January 2005 <http://www.cs.indiana.edu/~zmcmahon/biometrics-history.htm>.

[4] J. L. Wayman, "Biometrics – Now and Then: The development of biometrics over the last 40 years," H. Daum (ed.) Biometrics in the Reflection of Requirements: Second BSI Symposium on Biometrics 2004. SecuMedia, Bonn, 2004.

Introduction

"Biometrics" is a general term used alternatively to describe a characteristic or a process.

As a characteristic:

1. A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.

As a process:

2. Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Biometric systems have been researched and tested for a few decades, but have only recently entered into the public consciousness because of high profile applications, usage in entertainment media (though often not realistically) and increased usage by the public in day-to-day activities. Example deployments within the United States Government include the FBI's Integrated Automated Fingerprint Identification System (IAFIS), the US-VISIT program, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program. Many companies are also implementing biometric technologies to secure areas, maintain time records, and enhance user convenience. For example, for many years Disney World has employed biometric devices for season ticket holders to expedite and simplify the process of entering its parks, while ensuring that the ticket is used only by the individual to whom it was issued.

A typical biometric system is comprised of five integrated components: A **sensor** is used to collect the data and convert the information to a digital format. **Signal processing algorithms** perform quality control activities and develop the biometric template. A **data storage** component keeps information that new biometric templates will be compared to. A **matching algorithm** compares the new biometric template to one or more templates kept in data storage. Finally, a **decision process** (either automated or human-assisted) uses the results from the matching component to make a system-level decision.

Biometric Modalities

Commonly implemented or studied biometric modalities include fingerprint, face, iris, voice, signature and hand geometry. Many other modalities are in various stages of development and assessment. There is not one biometric modality that is best for all implementations. Many factors must be taken into account when implementing a biometric device including location, security risks, task (identification or verification), expected number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity.

Fingerprint Recognition

Manual comparison of fingerprints for recognition has been in use for many years, and has become an automated biometric identification technique over the past two decades. Fingerprints have an uneven surface of ridges and valleys that form a unique pattern for each individual. For most applications, the primary interest is in the ridge patterns on the top joint of the finger.

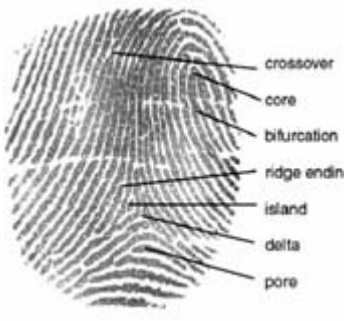


Figure 1: Fingerprint Recognition[1]

An important distinction to make is the difference between the FBI's IAFIS[2] system and the commercial fingerprint systems used for verification purposes. The FBI IAFIS system was developed to compare submitted fingerprint information against a database of several million fingerprints to determine if the individual has previously submitted fingerprints, and thus has a potential criminal history. IAFIS systems require information from all ten fingers, either ink-based or electronic, and preferably rolled impressions. Submitted fingerprints are compared against the fingerprints on file and are verified by 0, 1, or 2 fingerprint examiners. The process usually takes about two hours.

Commercial fingerprint systems that are used for verification purposes usually require only one finger to compare the fingerprint to the one on file to confirm the individual's claimed identity. This process is completely automated and usually takes less than a second. The two types of systems are not connected at all.

Face Recognition

Humans recognize familiar faces with considerable ease, but they are not good at recognizing unfamiliar individuals. Since the 1960s, machine vision researchers have been developing automated methods for recognizing individuals via their facial characteristics. Despite the volumes of research, there are no agreed-upon methods for automated face recognition as there are for fingerprints. Multiple approaches have existed for several years using low resolution 2D images. Recent work in high resolution 2D and 3D shows the potential to greatly improve face recognition accuracy.

Iris Recognition

The iris is the colored portion of an individual's eye. The concept of using the iris for recognition purposes dates back to 1936.[3] The next major advancement appeared in the late 1980s, with a patent being issued in 1994 for the algorithms that can perform iris recognition automatically. To obtain a good image of the iris, identification systems typically illuminate the iris with near-infrared light, which can be observed by most cameras yet is not detectable by, nor can it cause injury to, humans. A common misconception is that iris recognition shines a laser on the eye to "scan" it. This is incorrect untrue. Iris recognition simply takes an illuminated picture of the iris without causing any discomfort to the individual.

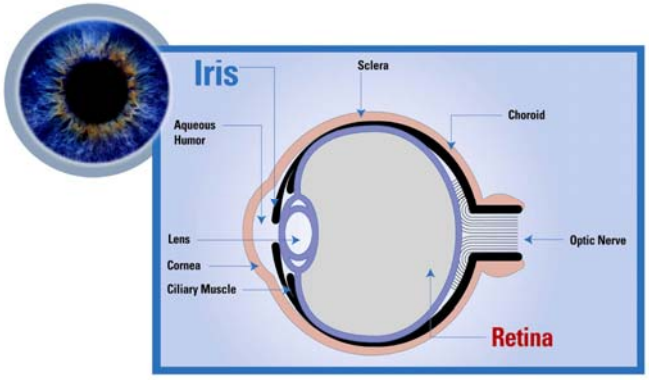


Figure 2: Iris Recognition.[4]

Hand/Finger Geometry

One of the first successful commercial biometric products was a hand geometry system. Typically, a user enters a PIN code to claim an identity, and then places his/her hand on the system,

which takes a picture of the hand. Using mirrors, the picture shows the view of the hand from the top and side. Measurements are then taken on the digits of the hand and compared to those collected at enrollment.

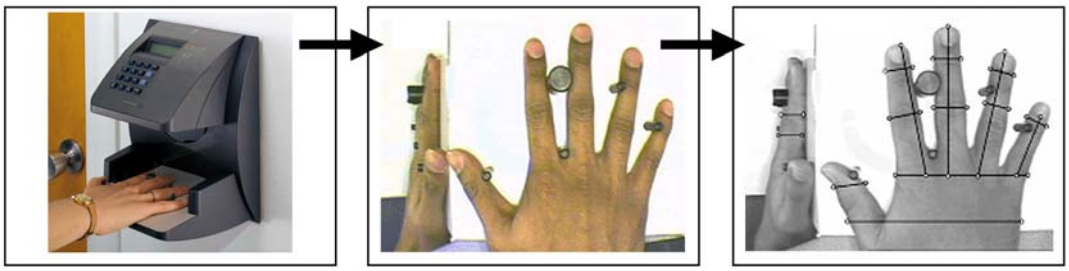


Figure 3: Hand Geometry.[5,6]

Other Biometric Identification Systems

Many other identification methods are in various stages of development and/or commercialization. Following are some examples.

- *Speaker recognition* uses an individual's speech, a feature influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual, for recognition purposes.
- *Dynamic Signature* measures the speed and pressure one uses when signing his or her name (not what the signature looks like).
- *Keystroke dynamics* measures the typing patterns of an individual.
- *Retina recognition* takes an image of the back of the eye and compares blood vessels with existing data.
- *Gait/Body recognition* measures how someone appears as he or she walks. As in face recognition, this technique is one that humans intuitively use to recognize someone.[7]
- *Facial Thermography* measures how heat dissipates off the face of an individual.

Testing and Statistics

The accuracy of a biometric system is determined through a series of tests, beginning with an assessment of matching algorithm accuracy (technology evaluation), then assessing performance in a mock environment (scenario evaluation), followed by live testing on site (operational evaluation) before full operations begin. Each evaluation serves a different purpose and involves different types of analyses.

Biometric terms, such as recognition, verification and identification, are sometimes used randomly. This is not only confusing, but incorrect as each term has a different meaning.

- Recognition is a generic term and does not necessarily imply either verification or identification. All biometric systems perform "recognition" to "again know" a person who has been previously enrolled.[2]
- Verification is a task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.
- Identification is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine if the person is in the database.

Because of these variances, different statistics must be used for each task.

Verification

False Acceptance Rate (FAR)

The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual's existing biometric. Example: Frank claims to be John and the system verifies the claim.

Verification Rate

The rate at which legitimate end-users are correctly verified.

Open-Set Identification (Watchlist)

False Alarm Rate

The percentage of times an alarm is incorrectly sounded on an individual who is not in the biometric system's database (the system alarms on Frank when Frank is not in the database), or an alarm is sounded but the wrong person is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

Detection and Identification Rate

The rate at which individuals who are in a database cause a system alarm and are properly identified in an open-set identification (watchlist) application.

Closed-set Identification

Identification Rate

The rate at which an individual in a database is correctly identified.

Standards

Standards help users deploy and maintain their systems in an easier manner, while also promoting longevity and enabling interoperability. There are numerous national and international efforts developing standards for:

- technical interfaces
- data interchange formats
- testing and reporting
- societal issues

Conclusion

The NSTC Subcommittee on Biometrics developed this introductory material in order to better communicate both within the government and with other interested parties. Stating facts and discussing related issues in a consistent, understandable manner, will enable smoother integration of privacy-protective biometric solutions. Federal agencies are working to ensure that their outreach activities are consistent with, and occasionally reference, this suite of documents so that the public, press and Congress are able to easily understand their plans and discuss

them productively. The Subcommittee encourages other entities to also use and reference this material.

This document serves as a general introduction to the field of biometrics; other documents describe key items in more detail. These include:

- Biometrics Frequently Asked Questions
- Biometrics Glossary
- Biometrics History
- Biometrics Overview
- Biometrics Standards
- Dynamic Signature
- Face Recognition
- Fingerprint Recognition
- Hand Geometry
- Iris Recognition
- Palm Print Recognition
- Speaker Recognition
- Biometrics Testing and Statistics
- Vascular Pattern Recognition
- The Privacy of Biometrics

These documents are available at: http://www.biometricscatalog.org/NSTCSubcommittee.

Document References

[1] International Biometric Group <http://www.biometricgroup.com>.

[2] John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

[3] Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).

[4] James Wayman et al, Biometric Systems Technology, Design and Performance Evaluation (London: Springer, 2005).

[5] Maltoni, Davide, Maio, Jain, and Prabhakar, Handbook of Fingerprint Recognition (Springer: New York, 2005).

[6] Secugen Biometrics Solutions <http://www.secugen.com/images/faq02.gif>.

[7] Biometrics: Department of Defense, "Biometrics 101"

<http://www.biometrics.dod.mil/bio101/assets/images/bio101/fingerprint_diagram.jpg>.

[8] Manfred Bromba, "Bioidentification: Frequently Asked Questions" <http://www.bromba.com/faq/fpfaqe.htm#Fingerprint-Sensoren>.

[9] Anil K. Jain, Ruud Bolle, and Sharath Pankanti, Personal Identification in a Networked Society (Kluwer Academic Publishing: Massachusetts, 1999).

National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Dynamic Signature

Introduction

"Dynamic Signature" is a biometric modality that uses, for recognition purposes, the anatomic and behavioral characteristics that an individual exhibits when signing his or her name (or other phrase). [1,2.] Dynamic Signature devices should not be confused with electronic signature capture systems that are used to capture a graphic image of the signature and are common in locations where merchants are capturing signatures for transaction authorizations.

Data such as the dynamically captured direction, stroke, pressure, and shape of an individual's signature can enable handwriting to be a reliable indicator of an individual's identity (i.e., measurements of the captured data, when compared to those of matching samples, are a reliable biometric for writer identification.)

History

The first signature recognition system was developed in 1965.[3] Dynamic signature recognition research continued in the 1970s focusing on the use of static or geometric characteristics (what the signature looks like) rather than dynamic characteristics (how the signature was made).[4] Interest in dynamic characteristics surged with the availability of better acquisition systems accomplished through the use of touch sensitive technologies.[4,5] In 1977, a patent was awarded for a "personal identification apparatus" that was able to acquire dynamic pressure information.[6]

Approach

Dynamic signature recognition uses multiple characteristics in the analysis of an individual's handwriting. These characteristics vary in use and importance from vendor to vendor and are collected using contact sensitive technologies, such as PDAs or digitizing tablets.[5]

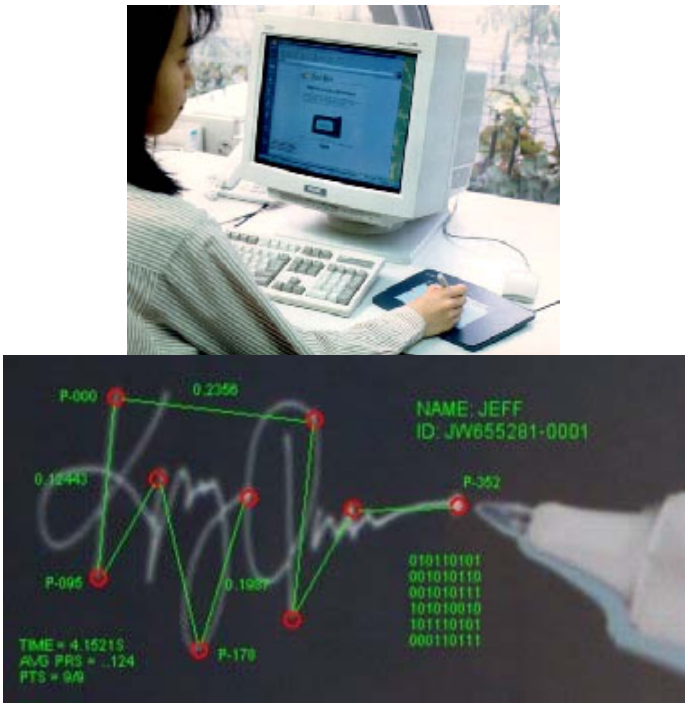


Figure 1: Dynamic Signature Depiction: As an individual signs the contact sensitive tablet, various measurements are observed and processed for comparison.[1,2]

Most of the features used are dynamic characteristics rather than static and geometric characteristics, although some vendors also include these characteristics in their analyses. Common dynamic characteristics include the velocity, acceleration, timing, pressure, and direction of the signature strokes, all analyzed in the X, Y, and Z directions. Figure 2 illustrates these recorded dynamic characteristics of a signature. The X and Y position are used to show the changes in velocity in the respective directions (indicated by the white and yellow lines) while the Z direction (red line) is used to indicate changes in pressure with respect to time.

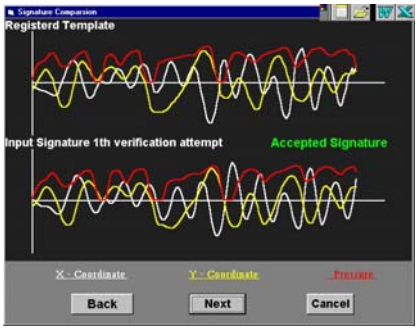


Figure 2: Graphic Depiction of Dynamic Signature Characteristics.[1]

Some dynamic signature recognition algorithms incorporate a learning function to account for the natural changes or drifts that occur in an individual's signature over time.[1]

The characteristics used for dynamic signature recognition are almost impossible to replicate. Unlike a graphical image of the signature, which can be replicated by a trained human forger, a computer manipulation, or a photocopy, dynamic characteristics are complex and unique to the handwriting style of the individual. Despite this major strength of dynamic signature recognition, the characteristics historically have a large intra-class variability (meaning that an individual's own signature may vary from collection to collection), often making dynamic signature recognition difficult. Recent research has reported that static writing samples can be successfully analyzed to overcome this issue.

United States Government Evaluations

In 1991, the Sandia National Laboratories produced A Performance Evaluation of Biometric Identification Devices (http://infoserve.sandia.gov/cgi-bin/techlib/access-control.pl/1991/910276.pdf), a report that evaluates the relative performance of multiple biometric devices, including dynamic signature.[7] In 1999, "Report of Biometrics In-House Test (http://www.epa.gov/cdx/cromerrr/propose/biometric_dmr-rpt.pdf)," an operational pilot in New York State sponsored by the Environmental Protection Agency[7], evaluated the interoperability of signature recognition hardware with existing user drivers and operating systems[8] and found numerous interoperability problems. Even though these tests represent the most recent government evaluations of notable scale, the information cannot be considered conclusive because of the age of the tests.

Standards Overview

Numerous activities regarding the interoperability of biometrics are ongoing at both the national and international level. On the national level, ANSI INCITS 395-2005 specifies a data interchange format for representation of digitized sign or signature data, for the purposes of biometric enrollment, verification or identification through the use of Raw Signature/Sign Sample Data or Common Feature Data. The data interchange format is generic, in that it may be applied and used in a wide range of

application areas where electronic signs or signatures are involved. No application-specific requirements or features are addressed in this standard.[9] At the international level, there are two corresponding documents currently in draft format: ISO/IEC FCD 19794-7: Information technology – Biometric data interchange formats – Part 7: Signature/sign time series data[10] and ISO/IEC WD 19794-11: Information technology – Biometric data interchange formats – Part 11: Signature/Sign Processed Dynamic Data.[11]

Summary

Dynamic signature verification is a biometric that can be easily integrated into existing systems because of the availability and prevalence of signature digitizers and the public's acceptance of the characteristic collection. On the downside, signature recognition can only be used for verification purposes and intra-class variability can cause non-ideal performance for some applications. A need for continued improvements in current products will help drive the development and application of this technology.

Document References

[1] "Biometric Signature Verification," Cyber-SIGN <http://www.cybersign.com/techoverview_what.htm>.

[2] "Signature Recognition," GAITS: Global Analytic Information Technology Services 8 August 2005 <http://www.gaits.com/biometrics_signature.asp>.

[3] A. J. Mauceri, "Feasibility Studies of Personal Identification by Signature Verification," Report no. SID 65 24 RADC TR 65 33, Space and Information System Division, North American Aviation Co., Anaheim, USA, 1965.

[4] G. Lorrette, "Handwriting Recognition or Reading? Situation at the Dawn of the 3rd Millennium," Universite de Rennesl, Advances in Handwriting Recognition, ed. Seong-Whan Lee (Singapore: World Scientific Publishing, 1999) 4-5.

[5] Marc Gaudreau, "On the Distinction between Biometric and Digital Signatures," CIC Enterprise Solutions <http://www.cic.com/enterprise/whitepapers/whitepaper5.asp>.

[6] John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins. Biometrics (New York: McGraw Hill Osborne, 2003).

[7] James Holmes, Larry Wright, and Russell Maxwell, "A Performance Evaluation of Biometric Identification Devices," Sandia National Laboratories 1991 <http://infoserve.sandia.gov/cgi-bin/techlib/access-control.pl/1991/910276.pdf>.

[8] "Report of Biometric In-house Test" 30 September 1999 <http://www.epa.gov/cdx/cromerrr/propose/biometric_dmr-rpt.pdf>.

[9] ANSI INCITS 395-2005, Information technology - Biometric Data Interchange Formats - Signature/Sign Data, 2005.

[10] ISO/IEC FCD 19794-7: Information technology – Biometric data interchange formats – Part 7: Signature/sign time series data.

[11] ISO/IEC WD 19794-11: Information technology – Biometric data interchange formats – Part 11: Signature/Sign Processed Dynamic Data.

Face Recognition

Introduction

Humans often use faces to recognize individuals and advancements in computing capability over the past few decades now enable similar recognitions automatically. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Major advancements and initiatives in the past ten to fifteen years have propelled face recognition technology into the spotlight. Face recognition can be used for both verification and identification (open-set and closed-set).

History

Automated face recognition is a relatively new concept. Developed in the 1960s, the first semi-automated system for face recognition required the administrator to locate features (such as eyes, ears, nose, and mouth) on the photographs before it calculated distances and ratios to a common reference point, which were then compared to reference data. In the 1970s, Goldstein, Harmon, and Lesk[1] used 21 specific subjective markers such as hair color and lip thickness to automate the recognition. The problem with both of these early solutions was that the measurements and locations were manually computed. In 1988, Kirby and Sirovich applied principle component analysis, a standard linear algebra technique, to the face recognition problem. This was considered somewhat of a milestone as it showed that less than one hundred values were required to accurately code a suitably aligned and normalized face image.[2] In 1991, Turk and Pentland discovered that while using the eigenfaces techniques, the residual error could be used to detect faces in images[3] – a discovery that enabled reliable real-time automated face recognition systems. Although the approach was somewhat constrained by environmental factors, it nonetheless created significant interest in furthering development of automated face recognition technologies.[3] The technology first captured the public's attention from the media reaction to a trial implementation at the January 2001 Super Bowl, which captured surveillance images and compared them to a database of digital mugshots. This demonstration initiated much-needed analysis on how to use the technology to support national needs while being

considerate of the public's social and privacy concerns. Today, face recognition technology is being used to combat passport fraud, support law enforcement, identify missing children, and minimize benefit/identity fraud.

Predominant Approaches

There are two predominant approaches to the face recognition problem: geometric (feature based) and photometric (view based). As researcher interest in face recognition continued, many different algorithms were developed, three of which have been well studied in face recognition literature: Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM).

PCA: Principal Components Analysis (PCA)

PCA, commonly referred to as the use of eigenfaces, is the technique pioneered by Kirby and Sirivich in 1988. With PCA, the probe and gallery images must be the same size and must first be normalized to line up the eyes and mouth of the subjects within the images. The PCA approach is then used to reduce the dimension of the data by means of data compression basics[2] and reveals the most effective low dimensional structure of facial patterns. This reduction in dimensions removes information that is not useful[4] and precisely decomposes the face structure into orthogonal (uncorrelated) components known as eigenfaces. Each face image may be represented as a weighted sum (feature vector) of the eigenfaces, which are stored in a 1D array. A probe image is compared against a gallery image by measuring the distance between their respective feature vectors. The PCA approach typically requires the full frontal face to be presented each time; otherwise the image results in poor performance.[4] The primary advantage of this technique is that it can reduce the data needed to identify the individual to 1/1000th of the data presented.[5]

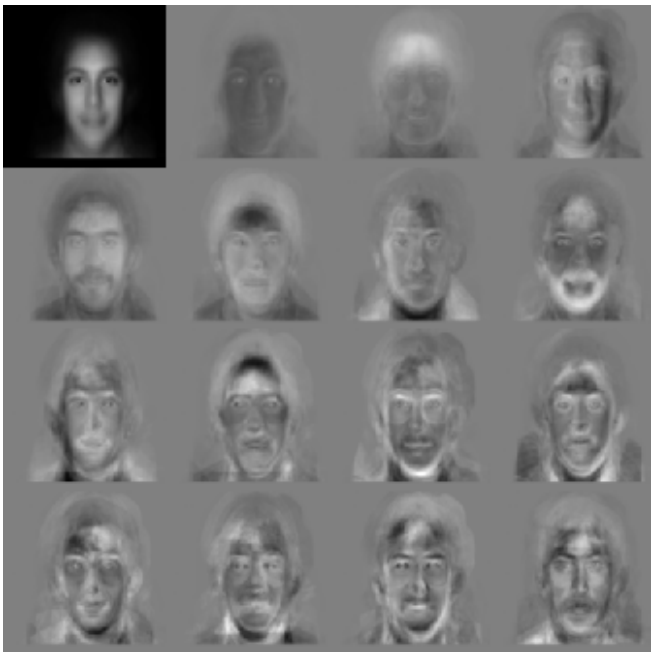


Figure 1: Standard Eigenfaces: Feature vectors are derived using eigenfaces.[6]

LDA: Linear Discriminant Analysis

LDA is a statistical approach for classifying samples of unknown classes based on training samples with known classes.[4] (Figure 2) This technique aims to maximize between-class (i.e., across users) variance and minimize within-class (i.e., within user) variance. In Figure 2 where each block represents a class, there are large variances between classes, but little variance within classes. When dealing with high dimensional face data, this technique faces the small sample size problem that arises where there are a small number of available training samples compared to the dimensionality of the sample space.[7]

Figure 2: Example of Six Classes Using LDA [8]

EBGM: Elastic Bunch Graph Matching

EBGM relies on the concept that real face images have many non-linear characteristics that are not addressed by the linear analysis methods discussed earlier, such as variations in illumination (outdoor lighting vs. indoor fluorescents), pose (standing straight vs. leaning over) and expression (smile vs. frown). A Gabor wavelet transform creates a dynamic link architecture that projects the face onto an elastic grid.[4] The Gabor jet is a node on the elastic grid, notated by circles on the image below, which describes the image behavior around a given pixel. It is the result of a convolution of the image with a Gabor filter, which is used to detect shapes and to extract features using image processing. [A convolution expresses the amount of overlap from functions, blending the functions together.] Recognition is based on the similarity of the Gabor filter response at each Gabor node.[4] This biologically-based method using Gabor filters is a process executed in the visual cortex of higher mammals. The difficulty with this method is the requirement of accurate landmark localization, which can sometimes be achieved by combining PCA and LDA methods.[4]

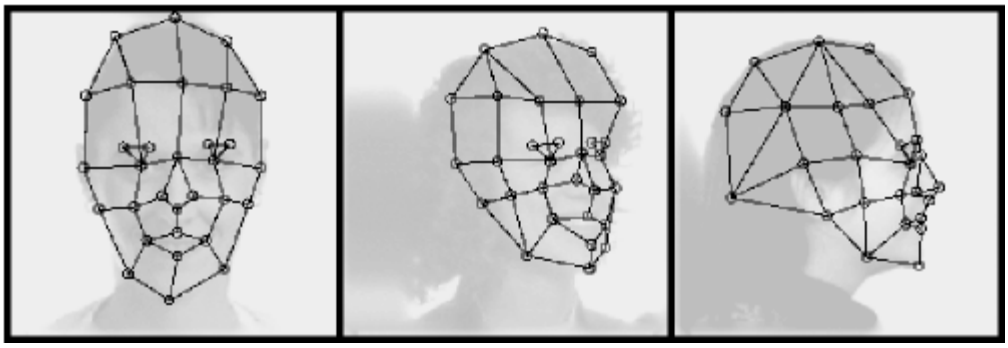


Figure 4: Elastic Bunch Map Graphing.[9]

United States Government Evaluations

The US Government has performed multiple evaluations to determine the capabilities and limitations of face recognition, and to encourage and direct future development. The FacE REcognition Technology (FERET) Evaluation, sponsored from 1993-1997 by the Defense Advanced Research Products Agency (DARPA),[10] was an effort to encourage the development of face recognition algorithms and technology by assessing the prototypes of face recognition systems. It propelled face recognition from its infancy to a market of commercial products.

The Face Recognition Vendor Tests (FRVT) were performed in 2000 and 2002, and another is planned for 2006. These evaluations built upon the work of FERET and coincided with the general onset of commercially available face recognition products. FRVT 2000[11] had two goals:

- Assess the capabilities of commercially available facial recognition systems; and
- Educate the biometrics community and the general public on how to properly present and analyze results.

FRVT 2002[12] was designed to measure technical progress since 2000, to evaluate performance on real-life large-scale databases, and to introduce new experiments to help better understand face recognition performance better. The FRVT 2002 included experiments with error bars, showing variances in performance as similar images were interchanged. Key FRVT 2002 results are:

- Given reasonable controlled indoor lighting, the current state of the art in face recognition is 90% verification at a 1% false accept rate.
- The use of morphable models, which maps a 2D image onto a 3D grid in an attempt to overcome lighting and pose variations, can significantly improve non-frontal face recognition.
- Watch list performance decreases as a function of gallery size – performance using smaller watch lists is better than performance using larger watch lists.
- In face recognition applications, accommodations should be made for demographic information since characteristics such as age and sex can significantly affect performance.

The goal of the Face Recognition Grand Challenge (FRGC) — the next step in the government development and evaluation process — is to promote and advance face recognition technology designed to support existing face recognition efforts of the US Government.[13] The FRGC will attempt to develop new face recognition techniques and develop prototype systems while increasing performance by an order of magnitude. The FRGC is open to face recognition researchers and developers in companies, academia, and research institutions. Soon after the completion of the FRGC, the Government will perform an in-depth assessment of face recognition — the FRVT 2006.

Standards Overview

Standardization is a vital portion of the advancement of the market and state of the art. Much work is being done at both the national and international standard organization levels to facilitate the interoperability and data interchange formats, which will help facilitate technology improvement on a standardized platform. The ANSI/INCITS (M1) 385-2004 and ISO SC37 19794-5 Face Recognition Data Interchange Format[14] are the major face recognition standards and address detailed human examination of face images, human verification of identity, and automated face identification and verification. These standards allow for interoperability among face recognition vendors.[15] The standards have established a defined frontal image[15] and are broken into subsections addressing full-frontal and token images. (A full-frontal image is defined as an image within five degrees from the center. A token image is defined by the location of the eyes.) These standards leave other images, such as semi-profile, undefined[15] but ensure that enrolled images will meet a quality standard needed for both automated face recognition and human inspection of face images.[14] Work is underway at both the national and international levels to update the standards for 3D face data. ANSI NIST ITL 1-2000 is also being updated to include more/better information for Type-10 face images. There is also related work at the international level to provide guidance to photographers on how to best capture face images for automated recognition. These standards also facilitate the use of face information in applications that have limited storage (e.g., passports, visas, driver's licenses).

Other standards, such as INCITS 398-2005 Common Biometric Exchange Formats Framework (CBEFF), deal specifically with the data elements used to describe the biometric data in a common way. The INCITS 358-2002 BioAPI Specification defines the Application Programming Interface and Service Provider Interface for a standard biometric technology interface. National and international standards organizations continue to work on the progression of standards in a direction that facilitates growth, advancement, and interoperability.

Summary

The computer-based face recognition industry has made much useful advancement in the past decade; however, the need for

higher accuracy systems remains. Through the determination and commitment of industry, government evaluations, and organized standards bodies, growth and progress will continue, raising the bar for face recognition technology.

Document References

[1] A. J. Goldstein, L. D. Harmon, and A. B. Lesk, "Identification of Human Faces," Proc. IEEE, May 1971, Vol. 59, No. 5, 748-760.

[2] L. Sirovich and M. Kirby, "A Low-Dimensional Procedure for the Characterization of Human Faces," J. Optical Soc. Am. A, 1987, Vol. 4, No.3, 519-524.

[3] M. A. Turk and A. P. Pentland, "Face Recognition Using Eigenfaces," Proc. IEEE, 1991, 586-591.

[4] D. Bolme, R. Beveridge, M. Teixeira, and B. Draper, "The CSU Face Identification Evaluation System: Its Purpose, Features and Structure," International Conference on Vision Systems, Graz, Austria, April 1-3, 2003. (Springer-Verlag) 304-311.

[5] "Eigenface Recognition" <http://et.wcu.edu/aidc/BioWebPages/eigenfaces.htm>.

[6] MIT Media Laboratory Vision and Modeling Group, "Photobook/Eigenfaces Demo" 25 July 2002 <http://vismod.media.mit.edu/vismod/demos/facerec/basic.html>.

[7] J. Lu, K.N. Plataniotis, and A.N. Venetsanopoulos, "Regularized Discriminant Analysis For the Small Sample Size Problem in Face Recognition," Pattern Recognition Letters, December 2003, Vol. 24, Issue 16: 3079-3087.

[8] Juwei Lu, "Boosting Linear Discriminant Analysis for Facial Recognition," 2002.

[9] Laurenz Wiskott, "Face Recognition by Elastic Bunch Graph Matching, " 24 April 1996 <http://www.neuroinformatik.ruhr-uni-bochum.de/ini/VDM/research/computerVision/graphMatching/identification/faceRecognition/contents.html>.

[10] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET Evaluation Methodology for Face-Recognition Algorithms," IEEE Transactions on PAMI, 2000, Vol. 22, No. 10: 1090-1104.

[11] D. M. Blackburn, J. M. Bone, and P. J. Phillips, "Facial Recognition Vendor Test 2000 Evaluation Report," February 2001 <http://www.frvt.org>.

[12] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, "Face Recognition Vendor Test 2002 Overview and Summary," March 2003 <http://www.frvt.org>.

[13] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the Face Recognition Grand Challenge," Proc. Computer Vision and Pattern Recognition Conference, San Diego, 2005.

[14] "Information technology – Biometric data interchange formats – Part 5: Face image data." Documents ISO/IEC 19794-5:2005, 2004 <http://www.iso.org/>.

[15] "Information Technology - Face Recognition Format for Data Interchange," document 385-2004 ANSI INCITS, 2004 <http://www.incits.org/>.

Fingerprint Recognition

Introduction

Fingerprint identification is one of the most well-known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

History

The practice of using fingerprints as a method of identifying individuals has been in use since the late nineteenth century when Sir Francis Galton defined some of the points or characteristics from which fingerprints can be identified. These "Galton Points" are the foundation for the science of fingerprint identification, which has expanded and transitioned over the past century. Fingerprint identification began its transition to automation in the late 1960s along with the emergence of computing technologies. With the advent of computers, a subset of the Galton Points, referred to as minutiae, has been utilized to develop automated fingerprint technology.

In 1969, there was a major push from the Federal Bureau of Investigation (FBI) to develop a system to automate its fingerprint identification process, which had quickly become overwhelming and required many man-hours for the manual process. The FBI contracted the National Bureau of Standards (NBS), now the National Institute of Standards and Technology (NIST), to study the process of automating fingerprint classification, searching, and matching.[1] NIST identified two key challenges: 1 scanning fingerprint cards and extracting minutiae from each fingerprint and 2 searching, comparing, and matching lists of minutiae against large repositories of fingerprints.

In 1975, the FBI funded the development of fingerprint scanners for automated classifiers and minutiae extraction technology, which led to the development of a prototype reader. This early reader used capacitive techniques to collect the fingerprint minutiae (See Hardware section).[2] At that time, only the

individual's biographical data, fingerprint classification data, and minutiae were stored because the cost of storage for the digital images of the fingerprints was prohibitive.[1]

Over the next few decades, NIST focused on and led developments in automatic methods of digitizing inked fingerprints and the effects of image compression on image quality, classification, extraction of minutiae, and matching.[3] The work at NIST led to the development of the M40 algorithm, the first operational matching algorithm used at the FBI[1] for narrowing the human search. The results produced by the M40 algorithm were provided to trained and specialized human technicians who evaluated the significantly smaller set of candidate images. The available fingerprint technology continued to improve and by 1981, five Automated Fingerprint Identification Systems (AFIS) had been deployed.[1] Various state systems within the US and other countries had implemented their own standalone systems, developed by a number of different vendors. During this evolution, communication and information exchange between the systems were overlooked, meaning that a fingerprint collected on one system could not be searched against another system.[1] These oversights led to the need for and development of fingerprint standards.

As the need for an integrated identification system within the US criminal justice community quickly became apparent, the next stage in fingerprint automation occurred at the end of the Integrated Automated Fingerprint Identification System (IAFIS) competition in 1994. The competition identified and investigated three major challenges: 1 digital fingerprint acquisition, 2 local ridge characteristic extraction, and 3 ridge characteristic pattern matching.[4] Demonstrated model systems were evaluated based on specific performance requirements. Lockheed Martin was selected to build the AFIS segment of the FBI's IAFIS project and the major IAFIS components were operational by 1999.[3] Also in this timeframe, commercial fingerprint verification products began to appear for various access control, logon, and benefit verification functions.

Approach

Concept

A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space

and are the low, shallow portion of the friction ridge skin. Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path. The images below present examples of fingerprint features: (a) two types of minutiae and (b) examples of other detailed characteristics sometimes used during the automatic classification and minutiae extraction processes.

The types of information that can be collected from a fingerprint's friction ridge impression include the flow of the friction ridges (Level 1 Detail), the presence or absence of features along the individual friction ridge paths and their sequence (Level 2 Detail), and the intricate detail of a single ridge (Level 3 Detail). Recognition is usually based on the first and second levels of detail or just the latter.

AFIS technology exploits some of these fingerprint features. Friction ridges do not always flow continuously throughout a pattern and often result in specific characteristics such as ending ridges, dividing ridges and dots, or other information. An AFIS is designed to interpret the flow of the overall ridges to assign a fingerprint classification and then extract the minutiae detail – a subset of the total amount of information available yet enough information to effectively search a large repository of fingerprints.

Figure 1: Minutiae.[5]

Figure 2: Other Fingerprint Characteristics.[6]

Hardware

A variety of sensor types — optical, capacitive, ultrasound, and thermal — are used for collecting the digital image of a fingerprint surface. Optical sensors take an image of the fingerprint, and are the most common sensor today. The

capacitive sensor determines each pixel value based on the capacitance measured, made possible because an area of air (valley) has significantly less capacitance than an area of finger (friction ridge skin). Other fingerprint sensors capture images by employing high frequency ultrasound or optical devices that use prisms to detect the change in light reflectance related to the fingerprint. Thermal scanners require a swipe of a finger across a surface to measure the difference in temperature over time to create a digital image.[7]

Software

The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching. Pattern matching simply compares two images to see how similar they are. Pattern matching is usually used in fingerprint systems to detect duplicates. The most widely used recognition technique, minutiae-based matching, relies on the minutiae points described above, specifically the location and direction of each point.[4]

United States Government Evaluations

As mandated by the USA PATRIOT ACT and the Enhanced Border Security Act, NIST managed the Fingerprint Vendor Technology Evaluation (FpVTE) to evaluate the accuracy of fingerprint recognition systems.[8] FpVTE was designed to assess the capability of fingerprint systems to meet requirements for both large-scale and small-scale real world applications. FpVTE 2003 consists of multiple tests performed with combinations of fingers (e.g., single fingers, two index fingers, four to ten fingers) and different types and qualities of operational fingerprints (e.g., flat livescan images from visa applicants, multi-finger slap livescan images from present-day booking or background check systems, or rolled and flat inked fingerprints from legacy criminal databases).

The most accurate systems in FpVTE 2003 were found to have consistently very low error rates across a variety of data sets. The variables that had the clearest effect on system accuracy were the number of fingers used and fingerprint quality. An increased number of fingers resulted in higher accuracy: the accuracy of searches using four or more fingers was better than the accuracy of two-finger searches, which was better than the accuracy of single-finger searches.

Standards Overview

Currently ongoing at both the national and international levels, fingerprints standards development is an essential element in fingerprint recognition because of the vast variety of algorithms and sensors available on the market. Interoperability is a crucial aspect of product implementation, meaning that images obtained by one device must be capable of being interpreted by a computer using another device. Major standards efforts focus on the standardization of the content, meaning, and representation of the fingerprint data interchange formats[9] and include the ANSI/INCITS 381-2004 Finger Image-Based Data Interchange Format, ANSI/INCITS 377-2004 Finger Pattern Based Interchange Format, ANSI-INCITS 378-2004 Finger Minutiae Format for Data Interchange, ISO/IEC 19794-2 Finger Minutiae Format for Data Interchange, ISO/IEC FCD 19794-3 Finger Pattern Based Interchange Format, and the ISO/IEC 19794-4 Finger Image Based Interchange Format.[10] (Additional information regarding these standards can be found in the Appendix.)

Another noteworthy standard is ANSI NIST ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information. This standard specifies a common format used for the exchange of fingerprint, facial, scar, mark and tattoo data effectively across jurisdictional lines or between dissimilar systems made by different manufacturers. Electronic Fingerprint Transmission Specification (v7.1) and Electronic Biometric Transmission Specification (v1.0) are specific implementations of ANSI NIST ITL 1-2000 used by the FBI and DoD. Other standards also associated with ANSI NIST ITL 1-2000 are the FBI's Wavelet Scalar Quantization (WSQ) and Join Photographic Experts Group 2000 (JPEG2000) which are both used for the compression of fingerprint images.

Notable US Government Fingerprint Programs

Fast Capture of Rolled-Equivalent Fingerprints and Palm Prints

Fast capture, a multi-agency Government initiative, is expanding fingerprint and palm research, challenging industry to develop and demonstrate technology to capture 10 rolled-equivalent fingerprints in less than 15 seconds and/or both palm prints in less than one minute, significantly improve fingerprint image quality, reduce the failure-to-enroll rate, and be affordable, rugged,

portable, relatively unobtrusive in size, and deployable in the near future.[11]

Integrated Automatic Fingerprint Identification System (IAFIS)

Maintained by the FBI Criminal Justice Information Services (CJIS), IAFIS contains over 47 million subjects.[12] System capabilities include automated tenprint and latent fingerprint searches, electronic image storage, and electronic exchanges of fingerprints and responses. Through partnerships formed between the FBI and the law enforcement community, IAFIS became operational in 1999 to expedite fingerprint search requests that were being performed manually through human verification — a process that could take up to three months. IAFIS request results are returned within two hours for criminal inquiries and within 24 hours for civil inquiries.[12]

NIST Special Publication 800-76

NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, contains specifics for acquiring, formatting, and storing fingerprint images and templates for collecting and formatting facial images; and specifications for biometric devices used to collect and read fingerprint images. The publication specifies that two fingerprint be stored on the card as “minutia templates,” mathematical representations of fingerprint images.[13]

US-VISIT

The US-VISIT program is the centerpiece of the United States government's efforts to transform our nation's border management and immigration systems in a way that meets the needs and challenges of the 21st century. US-VISIT is part of a continuum of biometrically-enhanced security measures that begins outside U.S. borders and continues through a visitor's arrival to and departure from the US.

Most visitors experience US-VISIT's biometric procedures — digital, inkless fingerprints and digital photographs — upon entry to the US. In those cases where a visitor requires a visa, the Department of State collects the visitor's biometric and biographic information. When the visitor arrives in the US, US-VISIT procedures allow the Department of Homeland Security to determine whether the person applying for entry is the same person who was issued the visa by the Department of State.

Summary

For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. The determination and commitment of the fingerprint industry, government evaluations and needs, and organized standards bodies have led to the next generation of fingerprint recognition, which promises faster and higher quality acquisition devices to produce higher accuracy and more reliability. Because fingerprints have a generally broad acceptance with the general public, law enforcement, and the forensic science community, they will continue to be used with many governments' legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric.

Document References

[1] John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

[2] Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).

[3] James Wayman, et al, Biometric Systems Technology, Design and Performance Evaluation (London: Springer, 2005).

[4] Maltoni, Davide, Maio, Jain, and Prabhakar, Handbook of Fingerprint Recognition (Springer: New York, 2005).

[5] Secugen Biometrics Solutions <http://www.secugen.com/images/faq02.gif>.

[6] International Biometric Group <http://www.biometricgroup.com>.

[7] Manfred Bromba, "Bioidentification: Frequently Asked Questions" <http://www.bromba.com/faq/fpfaqe.htm#Fingerprint-Sensoren>.

[8] FpVTE 2003: "Fingerprint Vendor Technology Evaluation" 6 July 2004 < http://fpvte.nist.gov/>.

[9] International Committee for Information Technology Standards, "M1 Biometrics" <http://www.ncits.org/tc_home/m1.htm>.

[10] International Organization for Standardization, "JTC 1/ SC37 Biometrics Projects"

<http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=5537&scopelist=PROGRAMME>.

[11] NSTC Subcommittee on Biometrics, "Fingerprint Recognition Interagency Coordination Plan" January 2006.

[12] FBI IAFIS "Integrated Automated Fingerprint Identification System: What is it?" 30 June 2005 <http://www.fbi.gov/hq/cjisd/iafis.htm>.

[13] National Institute of Standards and Technology, Computer Security Division: Computer Security Resource Center, "Personal Identity Verification (PIV) of Federal Employees/Contractors" 24 March 2006 <http://csrc.nist.gov/piv-program/index.html>.

Appendix

ANSI/INCITS 381-2004 Finger Image Based Data Interchange Format — This standard specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of raw or processed image data containing detailed pixel information.

For more information, see the following: http://www.incits.org.

ANSI/INCITS 377-2004 Finger Pattern Based Interchange Format — This standard specifies an interchange format for the exchange of pattern-based fingerprint recognition data. It describes the conversion of a raw fingerprint image to a cropped and down-sampled finger pattern followed by the cellular representation of the finger pattern image to create the finger-pattern interchange data.

For more information, see the following: http://www.incits.org.

ANSI/INCITS 378-2004 Finger Minutiae Format for Data Interchange -- This standard defines a method of representing fingerprint information using the concept of minutiae. It defines the placement of the minutiae on a fingerprint, a record format for containing the minutiae data, and optional extensions for ridge count and core/delta information.

For more information, see the following: http://www.incits.org.

ANSI/NIST ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information — This

standard defines the content, format, and units of measurement for the exchange of fingerprint, palm print, facial/mugshot, and scar, mark, & tattoo (SMT) image information that may be used in the identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images.

For more information, see the following: ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf

ISO/IEC 19794-2 Finger Minutiae Format for Data Interchange – This standard describes how minutiae points shall be determined, defines data formats for containing the data for general and smart card use, and details conformance information. Guidelines and values for matching and decision parameters are provided as an informative Annex. The standard defines three types of minutiae, including ridge ending and ridge bifurcation. The adopted minutiae determination strategy relies on skeletons derived from a digital fingerprint image. For more information, see the following: http://www.iso.org.

ISO/IEC FCD 19794-3 Finger Pattern Based Interchange Format – This draft standard specifies that a fingerprint image is divided into a grid of overlapping or non-overlapping cells. At each cell, the finger pattern will be represented by a cell structure. A method to obtain the cell structure is to decompose each of the cells into a two-dimensional spectral representation such as the two-dimensional Discrete Fourier Transform (DFT). The decomposition produces spectral components, where each component can be characterized by a wavelength in the horizontal (x) and vertical (y) directions, amplitude, and a phase. For more information, see the following: http://www.iso.org.

ISO/IEC 19794- 4 Finger Image Based Interchange Format – This standard specifies that the image shall appear to have been captured in an upright position and shall be approximately centered horizontally in the field of view. The scanning sequence and recorded data shall appear to have been from left-to-right, progressing from top-to bottom of the fingerprint. The origin of the axes, pixel location (0,0), is at the upper left hand corner of each image with the x-coordinate (horizontal) position increasing positively from the origin to the right side of the image while the y-coordinate (vertical) position increasing positively from the origin to the bottom of the image. It also specifies that the

header must be CBEFF compliant. For more information, see the following: http://www.iso.org.

ISO/IEC 19794-8 Finger Pattern Skeletal Data – This standard it is intended to be used to achieve interoperability between pattern and minutiae-based fingerprint recognition systems. It is based on the common properties shared between the spectral pattern and minutia by encoding ridges in a manner that the skeleton of the ridge provides the basis for detecting a minutia.

For more information, see the following: http://www.iso.org.

EFTS v7.1 Electronic Fingerprint Transmission Specification – This specification covers electronic transmission of information involving fingerprints to the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS) based on the ANSI NIST ITL 1-2000 strandard. The purpose of this document is to specify certain requirements to which agencies must adhere to communicate electronically with the IAFIS. For more information, see http://www.fbi.gov/filelink.html?file=/hq/cjisd/iafis/efts71/efts71.pdf.

EBTS v1.0 Electronic Biometric Transmission Specification – This specification describes customizations of the Federal Bureau of Investigation (FBI) Electronic Fingerprint Transmission Specification (EFTS) transactions that are necessary to utilize the Department of Defense (DoD) Automated Biometric Identification System (ABIS).

FBI- WSQ (Wavelet Scalar Quantization) Fingerprint Image Compression – WSQ is a lossy compression that is able to preserve the high resolution details of gray scale images that are usually discarded by other lossy compression algorithms. It achieves high compression ratio, on average 15:1 depending on parameters. For more information, see the "Criminal Justice Information Services (CJIS) WSQ Gray-scale Fingerprint Image Compression Specification," Federal Bureau of Investigation, Document No. IAFIS-IC-0110 (V3), 19 December 1997.

JPEG2000 (Joint Photographic Experts Group 2000) – Fingerprint Image Compression is a new image coding system that uses state-of-the-art compression techniques based on wavelet technology. Its architecture should lend itself to a wide range of uses from portable digital cameras through to advanced pre-press, medical imaging and other key sectors.

National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Hand Geometry

Introduction

Hand geometry recognition is the longest implemented biometric type, debuting in the market in the late 1980s. The systems are widely implemented for their ease of use, public acceptance, and integration capabilities. One of the shortcomings of the hand geometry characteristic is that it is not highly unique, limiting the applications of the hand geometry system to verification tasks only.

History

Hand geometry systems have the longest implementation history of all biometric modalities. David Sidlauskas developed and patented the hand geometry concept in 1985[1] and the first commercial hand geometry recognition systems became available the next year.[2] The 1996 Olympic Games implemented hand geometry systems to control and protect physical access to the Olympic Village.[2] Many companies implement hand geometry systems in parallel with time clocks for time and attendance purposes. Walt Disney World has used a similar "finger" geometry technology system for several years to expedite and facilitate entrance to the park and to identify guests as season ticket holders to prevent season ticket fraud.[3]

Approach

The devices use a simple concept of measuring and recording the length, width, thickness, and surface area of an individual's hand while guided on a plate (Figure 1). Hand geometry systems use a camera to capture a silhouette image of the hand (Figure 2).

The hand of the subject is placed on the plate, palm down, and guided by five pegs that sense when the hand is in place.

Figure 1: Bottom View.[4]

The resulting data capture by a Charge-Coupled Device (CCD) camera of the top view of the hand including example distance measurements.

Figure 2: Silhouette of Hand Image.[4]

The image captures both the top surface of the hand and a side image that is captured using an angled mirror (Figure 3). Upon capture of the silhouette image, 31,000 points are analyzed and 90 measurements are taken; the measurements range from the length of the fingers, to the distance between knuckles, to the height or thickness of the hand and fingers (Figure 4).[2] This information is stored in nine bytes of data, an extremely low number compared to the storage needs of other biometric systems.[2]

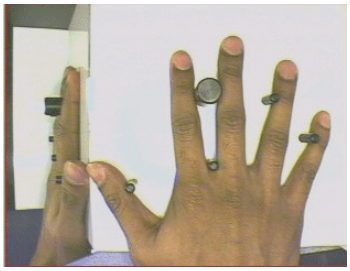


Figure 3: Hand Including Mirror Image as Seen by the CCD Camera.[5]

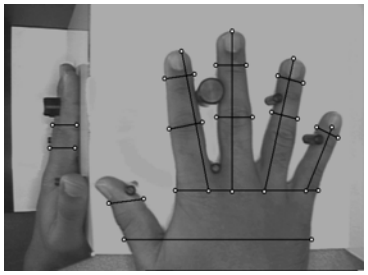


Figure 4: Example Distance Measurements.[5]

The enrollment process of a hand geometry system typically requires the capture of three sequential images of the hand, which are evaluated and measured to create a template of the user's characteristics. Upon the submission of a claim, the system recalls the template associated with that identity; the claimant places his/her hand on the plate; and the system captures an image and creates a verification template to compare to the template developed upon enrollment. A similarity score is produced and, based on the threshold of the system, the claim is either accepted or rejected.

United States Government Evaluations

The US government has sponsored two evaluations of hand geometry technology. The 1996 Evaluation of the INSPASS Hand Geometry Data determined the effect of a threshold on system operation[6], established false accept and false reject rates as a function of the threshold, and presented an estimate of the Receiver Operating Characteristics (ROC) curve for the INSPASS system.[6] The evaluators noted that an estimate was the best that could be achieved with the available data.[6] A 1991 Performance Evaluation of Biometric Identification Devices evaluated the relative performance of multiple biometric devices, including hand geometry.[7]

Standards Overview

Standards development efforts focusing on hand geometry technology, on both the national and international levels, are intended to accelerate the development of interoperable authentication-based security solutions. ANSI INCITS 396-2005 Hand Geometry Interchange Format defines the data interchange format for storing, recording, and transmitting hand geometry information collected from the hand silhouette.[8] It defines both content and format of the data for exchange as well as the units used for the measurement of the hand geometry data.[8] This national standard corresponds to ISO/IEC CD (Committee Draft) 19794-10 Biometric Interchange Format – Part 10, Hand Geometry Silhouette Data on the international standards level (ISO/IEC).[9] The international standard is still in draft format and has not yet been approved as an official standard.

Summary

Hand geometry recognition systems are widely used for applications in physical access, attendance tracking, and personal verification. They have found a sustainable market niche through use in security and accountability applications. Their ease of use, stand-alone capabilities, and small data requirements make them a popular choice for those in need of verification systems.

Document References

[1] United States Patent and Trademark Office, "Patent 4,736,203: 3D hand profile identification apparatus," 5 April 1988 >.

[2] IR Recognition Systems <http://recogsys.com/index.shtml>.

[3] "Finger Scanning at Disney Parks Causes Concern," 15 July 2005 <http://www.local6.com/news/4724689/detail.html>.

[4] "Hand Geometry and Handwriting," GlobalSecurity.org 27 April 2005 <http://www.globalsecurity.org/security/systems/hand.htm>.

[5] Arun Ross, Anil Jain, and Sharat Pankanti, "A Hand Geometry-Based Verification System" <http://biometrics.cse.msu.edu/hand_proto.html>.

[6] James Wayman, ed., "National Biometric Test Center Collected Works," San Jose State University, August 2000 <http://www.engr.sjsu.edu/biometrics/nbtccw.pdf>.

[7] James Holmes, Larry Wright, and Russell Maxwell, "A Performance Evaluation of Biometric Identification Devices," Sandia National Laboratories, June 1991

<http://infoserve.sandia.gov/cgi-bin/techlib/access-control.pl/1991/910276.pdf>.

[8] "Information Technology – Hand Geometry Format for Data Interchange," ANSI INCITS 396-2005 <http://www.ncits.org/scopes/1643.htm>.

[9] "Information Technology - Biometric data interchange formats – Part 10: Hand Geometry Silhouette Data," ISO/IEC CD 19794-10 <http://www.ncits.org>.




National Science and Technology Council (NSTC)

Committee on Technology

Committee on Homeland and National Security

Subcommittee on Biometrics

Introduction

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris (Figure 1). The automated method of iris recognition is relatively young, existing in patent only since 1994.[1]

The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle (Figure 2).

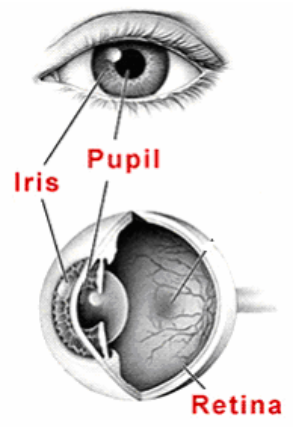


Figure 1: Iris Diagram[2]

Figure 2: Iris Structure.[3]

Although the coloration and structure of the iris is genetically linked, the details of the patterns are not. The iris develops during prenatal growth through a process of tight forming and folding of the tissue membrane.[4] Prior to birth, degeneration occurs, resulting in the pupil opening and the random, unique patterns of the iris.[5] Although genetically identical, an individual's irides are unique and structurally distinct, which allows for it to be used for recognition purposes.

History

In 1936, ophthalmologist Frank Burch proposed the concept of using iris patterns as a method to recognize an individual.[6] In 1985, Drs. Leonard Flom and Aran Safir, ophthalmologists, proposed the concept that no two irides are alike,[6] and were awarded a patent for the iris identification concept in 1987. Dr.

Flom approached Dr. John Daugman to develop an algorithm to automate identification of the human iris. In 1993, the Defense Nuclear Agency began work to test and deliver a prototype unit, which was successfully completed by 1995 due to the combined efforts of Drs. Flom, Safir, and Daugman. In 1994, Dr. Daugman was awarded a patent for his automated iris recognition algorithms. In 1995, the first commercial products became available.[7] In 2005, the broad patent covering the basic concept of iris recognition expired, providing marketing opportunities for other companies that have developed their own algorithms for iris recognition. The patent on the IrisCodes® implementation of iris recognition developed by Dr. Daugman (explained below) will not expire until 2011.[8]

Approach

Before recognition of the iris takes place, the iris is located using landmark features. These landmark features and the distinct shape of the iris allow for imaging, feature isolation, and extraction. Localization of the iris is an important step in iris recognition because, if done improperly, resultant noise (e.g., eyelashes, reflections, pupils, and eyelids) in the image may lead to poor performance.

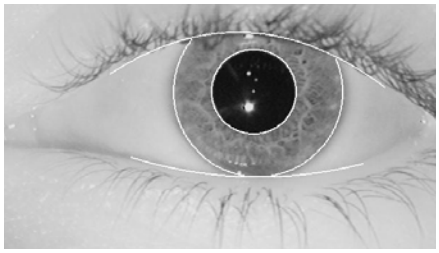


Figure 3: White outlines indicate the localization of the iris and eyelid boundaries.[3]

Iris imaging requires use of a high quality digital camera. Today's commercial iris cameras typically use infrared light to illuminate the iris without causing harm or discomfort to the subject.

Upon imaging an iris, a 2D Gabor wavelet filters and maps the segments of the iris into phasors (vectors). These phasors include information on the orientation and spatial frequency ("what" of

the image) and the position of these areas ("where" of the image).[9] This information is used to map the IrisCodes® (Figures 4 & 5).

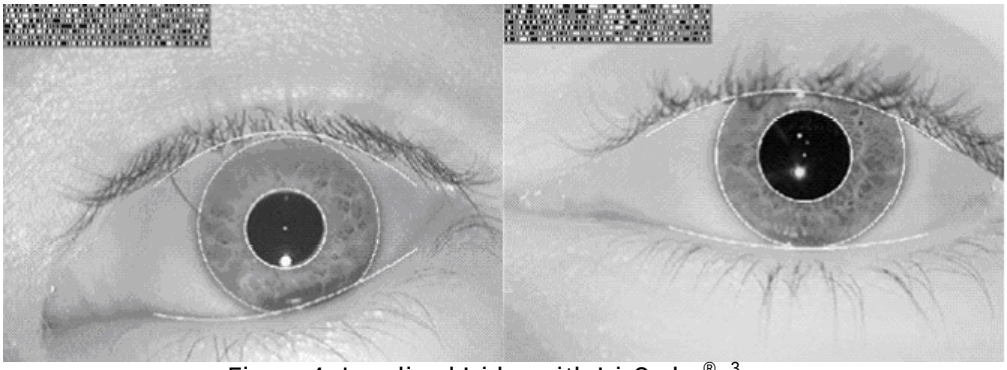


Figure 4: Localized Irides with IrisCodes®. [3]

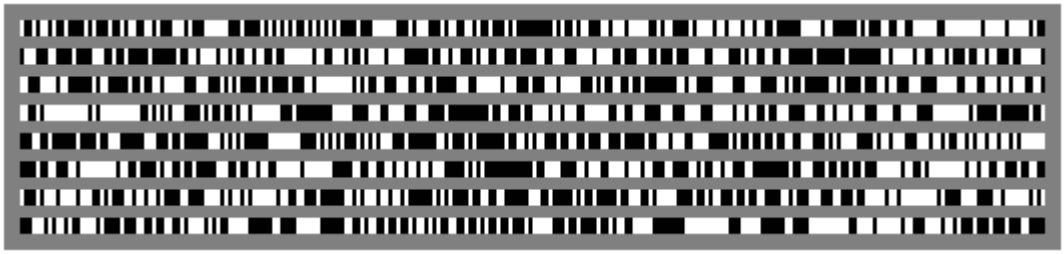


Figure 5: Pictorial Representation of IrisCode®. [3]

Iris patterns are described by an IrisCode® using phase information collected in the phasors. The phase is not affected by contrast, camera gain, or illumination levels. The phase characteristic of an iris can be described using 256 bytes of data using a polar coordinate system. Also included in the description of the iris are control bytes that are used to exclude eyelashes, reflection(s), and other unwanted data.[10]

To perform the recognition, two IrisCodes® are compared. The amount of difference between two IrisCodes® — Hamming Distance (HD) — is used as a test of statistical independence between the two IrisCodes®. If the HD indicates that less than one-third of the bytes in the IrisCodes® are different, the IrisCode® fails the test of statistical significance, indicating that the IrisCodes® are from the same iris. Therefore, the key concept to iris recognition is failure of the test of statistical independence.[10]

Iris vs. Retina Recognition

As discussed above, iris recognition utilizes the iris muscle to perform verification. Retinal recognition uses the unique pattern of blood vessels on an individual's retina at the back of the eye. The figure below illustrates the structure of the eye.

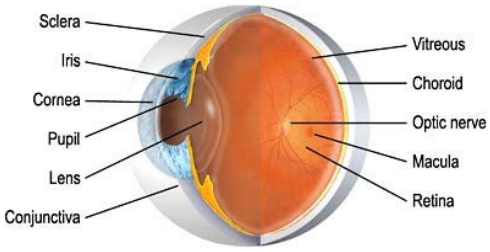


Figure 6: Structure of the Eye.[11]

Both techniques involve capturing a high quality picture of the iris or retina, using a digital camera. In the acquisition of these images, some form of illumination is necessary. Both techniques use NIR (near infrared) light. Although safe in a properly designed system, eye safety is a major concern for all systems that illuminate the eye. Because infrared has insufficient energy to cause photochemical effects, the principal potential damage modality is thermal. When NIR is produced using light emitting diodes, the resulting light is incoherent. Any risk for eye safety is remote with a single LED source using today's LED technology. Multiple LED illuminators can, however, produce eye damage if not carefully designed and used.

United States Government Evaluations

The US Department of Homeland Security (DHS) and the Intelligence Technology Innovation Center (ITIC) co-sponsored a test of iris recognition accuracy, usability, and interoperability referred to as the Independent Testing of Iris Recognition Technology (ITIRT) (http://www.biometricscatalog.org/itirt/ITIRT-FinalReport.pdf), the results of which were released in May 2005. The scenario test evaluated enrollment and matching software, and acquisition devices. The ITIRT's primary objective was to evaluate iris recognition performance in terms of match rates, enrollment and acquisition rates, and level of effort required from the user. The evaluation of match rates determined the

ability of algorithms to correctly match samples in a variety of intra-device and cross-device test cases based on genuine and impostor comparisons. The enrollment and acquisition evaluation determined the ability of the subject acquisition devices to successfully enroll IrisCodes® and acquire iris samples from test subjects. The level of effort evaluation determined the ability of these devices to acquire iris images and IrisCodes® from test subjects with minimal transaction durations and repeated attempts. ITIRT did not evaluate iris recognition systems in terms of availability, liveness detection, or ease of integration with external systems.[12]

The National Institute of Standards and Technology (NIST) is conducting the Iris Challenge Evaluation (ICE) (http://iris.nist.gov/ICE/), a two-phase large-scale independent development and technology evaluation of iris recognition technology to assess the current state of the art and to promote the development and advancement of iris recognition technology. Phase I will present an iris challenge problem while Phase II will measure the performance of the technology using a standard dataset and test methodology.[13]

Standards Overview

Current standards work in the area of iris recognition exists on the national and international level. The "ANSI/INCITS 379-2004 Iris Interchange Format"[15] and "ISO/IEC 19794-6: 2005 Biometric Data Interchange Format – Part 6: Iris image data"[15] standards are the major iris recognition standards and define two data formats for representing an iris image. The first format utilizes a rectilinear format in which the image can be raw or compressed and can vary in size based on field of view and compression or color (gray or color intensity levels).[14] The second format utilizes a polar image specification with specific preprocessing and segmentation steps for the image, which can be raw or compressed; contains only iris information; and is much more compact than the first.[16] These standards also define data structures and headers to support the storage of interoperable information[14] and will provide interoperability among vendors by providing a compact method of human iris representation. The current state of the technology allows for interoperability only through the transmission of the whole iris image, which requires storage of excess data and high bandwidth and introduces additional sources of errors through lengthy data transmissions processes.

Products must adhere to the illumination safety standards ANSI/IESNA RP-27.1-96 and IEC 60825-1 Amend.2, Class 1 LED, the latest worldwide standards in the illumination safety area, to ensure safe use of infrared technology.

Other standards, such as INCITS 398-2005 Common Biometric Exchange Formats Framework (CBEFF), deal specifically with the data elements used to describe the biometric data in a common way. Another standard is the INCITS 358-2002 BioAPI Specification that defines the Application Programming Interface and Service Provider Interface for a standard biometric technology interface. National and international standards organizations are working to continue the progression of the standards in a direction to facilitate growth, advancement, and interoperability.

Summary

Having only become automated and available within the past decade, the iris recognition concept and industry are still relatively new so a need for continued research and testing remains. Through the determination and commitment of industry, government evaluations, and organized standards bodies, growth and progress will continue, raising the bar for iris recognition technology.

Document References

[1] John Daugman, "Iris Recognition for Personal Identification," The Computer Laboratory, University of Cambridge <http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html>.

[2] University of Arkansas for Medical Science, "Information for Patients: Retina Services - Age-Related Macular Degeneration" <http://www.uams.edu/jei/patients/retina_services/maculardegen.asp>.

[3] John Daugman, "University of Cambridge: Computer Laboratory: Webpage for

John Daugman" <http://www.cl.cam.ac.uk/users/jgd1000/>.

[4] Mark Hill, "ANAT2310: Eye Development," The University of New South Wales, 2003 <http://anatomy.med.unsw.edu.au/cbl/teach/anat2310/Lecture06Senses(print).pdf>.

[5] Barbara Westmoreland, Michael Lemp, and Richard Snell, Clinical Anatomy of the Eye 2nd ed. (Oxford: Blackwell Science Inc., 1998).

[6] "Individual Biometrics: Iris Scan" 5 July 05, National Center for State Courts 6 July 06 <http://ctl.ncsc.dni.us/biomet%20web/BMIris.html>.

[7] Iridian Technologies, "Historical Timeline," 2003 <http://www.iridiantech.com/about.php?page=4>.

[8] Kelly Smith, "Iris Patent Question," Email to Jim Cambier 9 June 2005.

[9] International Biometric Group, "Iris Recognition Technology" <http://www.biometricgroup.com/reports/public/reports/iris-scan_tech.html>.

[10] John Daugman, "Mathematical Explanation of Iris Technologies" The Computer Laboratory, University of Cambridge <http://www.cl.cam.ac.uk/users/jgd1000/math.html>.

[11] "Eye Anatomy," St. Luke's Cataract & Laser Institute <http://www.stlukeseye.com/Anatomy.asp>.

[12] "Independent Testing of Iris Recognition Technology" May 2005 <http://www.biometricscatalog.org/itirt/itirt-FinalReport.pdf>.

[13] "Iris Challenge Evaluation," NIST: Information Access Division: Image Group 10 June 2005 <http://iris.nist.gov/ICE/>.

[14] "Information Technology – Iris Image Interchange Format," ANSI INCITS 379-2004, 2004.

[15] "Information Technology – Biometric data interchange formats – Part 6: Iris image data," ISO/IEC 19794-6:2005, 2005.

Palm Print Recognition

Introduction

Palm print recognition inherently implements many of the same matching characteristics that have allowed fingerprint recognition to be one of the most well-known and best publicized biometrics. Both palm and finger biometrics are represented by the information presented in a friction ridge impression. This information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis. The data represented by these friction ridge impressions allows a determination that corresponding areas of friction ridge impressions either originated from the same source or could not have been made by the same source. Because fingerprints and palms have both uniqueness and permanence, they have been used for over a century as a trusted form of identification. However, palm recognition has been slower in becoming automated due to some restraints in computing capabilities and live-scan technologies. This paper provides a brief overview of the historical progress of and future implications for palm print biometric recognition.

History

In many instances throughout history, examination of handprints was the only method of distinguishing one illiterate person from another since they could not write their own names. Accordingly, the hand impressions of those who could not record a name but could press an inked hand onto the back of a contract became an acceptable form of identification. In 1858, Sir William Herschel, working for the Civil Service of India, recorded a handprint on the back of a contract for each worker to distinguish employees from others who might claim to be employees when payday arrived. This was the first recorded systematic capture of hand and finger images that were uniformly taken for identification purposes.[1]

The first known AFIS system built to support palm prints is believed to have been built by a Hungarian company. In late 1994, latent experts from the United States benchmarked the palm system and invited the Hungarian company to the 1995 International Association for Identification (IAI) conference. The palm and fingerprint identification technology embedded in the palm system was subsequently bought by a US company in 1997.

In 2004, Connecticut, Rhode Island and California established statewide palm print databases that allowed law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders.[2,3]

Australia currently houses the largest repository of palm prints in the world. The new Australian National Automated Fingerprint Identification System (NAFIS) includes 4.8 million palm prints. The new NAFIS complies with the ANSI/NIST international standard for fingerprint data exchange, making it easy for Australian police services to provide fingerprint records to overseas police forces such as Interpol or the FBI, when necessary.[4]

Over the past several years, most commercial companies that provide fingerprint capabilities have added the capability for storing and searching palm print records. While several state and local agencies within the US have implemented palm systems, a centralized national palm system has yet to be developed. Currently, the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division houses the largest collection of criminal history information in the world. This information primarily utilizes fingerprints as the biometric allowing identification services to federal, state, and local users through the Integrated Automated Fingerprint Identification System (IAFIS). The Federal Government has allowed maturation time for the standards relating to palm data and live-scan capture equipment prior to adding this capability to the current services offered by the CJIS Division. The FBI Laboratory Division has evaluated several different commercial palm AFIS systems to gain a better understanding of the capabilities of various vendors. Additionally, state and local law enforcement have deployed systems to compare latent palm prints against their own palm print databases. It is a goal to leverage those experiences and apply them towards the development of a National Palm Print Search System.

In April 2002, a Staff Paper on palm print technology and IAFIS palm print capabilities was submitted to the Identification Services (IS) Subcommittee, CJIS Advisory Policy Board (APB). The Joint Working Group then moved "for strong endorsement of the planning, costing, and development of an integrated latent print capability for palms at the CJIS Division of the FBI. This should proceed as an effort along the same parallel lines that IAFIS was developed and integrate this into the CJIS technical capabilities…."[5]

As a result of this endorsement and other changing business needs for law enforcement, the FBI announced the Next Generation IAFIS (NGI) initiative. A major component of the NGI initiative is the development of the requirements for and deployment of an integrated National Palm Print Service. Law enforcement agencies indicate that at least 30 percent of the prints lifted from crime scenes — from knife hilts, gun grips, steering wheels, and window panes — are of palms, not fingers.[6] For this reason, capturing and scanning latent palm prints is becoming an area of increasing interest among the law enforcement community. The National Palm Print Service is being developed on the basis of improving law enforcement's ability to exchange a more complete set of biometric information, making additional identifications, quickly aiding in solving crimes that formerly may have not been possible, and improving the overall accuracy of identification through the IAFIS criminal history records.

Approach

Concept

Palm identification, just like fingerprint identification, is based on the aggregate of information presented in a friction ridge impression. This information includes the flow of the friction ridges (Level 1 Detail), the presence or absence of features along the individual friction ridge paths and their sequences (Level 2 Detail), and the intricate detail of a single ridge (Level 3 detail). To understand this recognition concept, one must first understand the physiology of the ridges and valleys of a fingerprint or palm. When recorded, a fingerprint or palm print appears as a series of dark lines and represents the high, peaking portion of the friction ridged skin while the valley between these ridges appears as a white space and is the low, shallow portion of the friction ridged skin. This is shown in Figure 1.

Figure 1: Fingerprint Ridges (Dark Lines) vs. Fingerprint Valleys (White Lines).

Palm recognition technology exploits some of these palm features. Friction ridges do not always flow continuously throughout a pattern and often result in specific characteristics such as ending ridges or dividing ridges and dots. A palm recognition system is designed to interpret the flow of the overall ridges to assign a classification and then extract the minutiae detail — a subset of the total amount of information available, yet enough information to effectively search a large repository of palm prints. Minutiae are limited to the location, direction, and orientation of the ridge endings and bifurcations (splits) along a ridge path. The images in Figure 2 present a pictorial representation of the regions of the palm, two types of minutiae, and examples of other detailed characteristics used during the automatic classification and minutiae extraction processes.

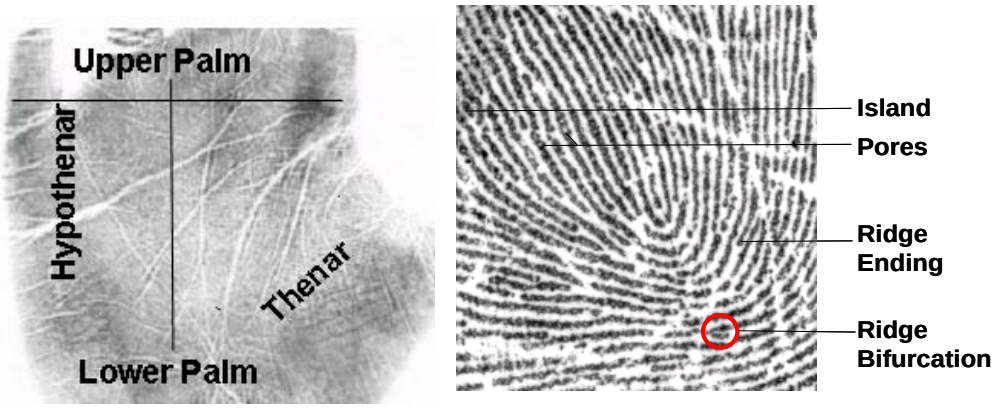


Figure 2: Palm Print and Close-up Showing Two Types of Minutiae and Other Characteristics.

Hardware

A variety of sensor types — capacitive, optical, ultrasound, and thermal — can be used for collecting the digital image of a palm surface; however, traditional live-scan methodologies have been slow to adapt to the larger capture areas required for digitizing palm prints. Challenges for sensors attempting to attain high-resolution palm images are still being dealt with today. One of the most common approaches, which employs the capacitive sensor, determines each pixel value based on the capacitance measured, made possible because an area of air (valley) has significantly less capacitance than an area of palm (ridge). Other palm sensors capture images by employing high frequency ultrasound or optical devices that use prisms to detect the change

in light reflectance related to the palm. Thermal scanners require a swipe of a palm across a surface to measure the difference in temperature over time to create a digital image. Capacitive, optical, and ultrasound sensors require only placement of a palm.

Software

Some palm recognition systems scan the entire palm, while others require the palms to be segmented into smaller areas to optimize performance. Maximizing reliability within either a fingerprint or palm print system can be greatly improved by searching smaller data sets. While fingerprint systems often partition repositories based upon finger number or pattern classification, palm systems partition their repositories based upon the location of a friction ridge area. Latent examiners are very skilled in recognizing the portion of the hand from which a piece of evidence or latent lift has been acquired. Searching only this region of a palm repository rather than the entire database maximizes the reliability of a latent palm search.

Like fingerprints, the three main categories of palm matching techniques are minutiae-based matching, correlation-based matching, and ridge-based matching. Minutiae-based matching, the most widely used technique, relies on the minutiae points described above, specifically the location, direction, and orientation of each point. Correlation-based matching involves simply lining up the palm images and subtracting them to determine if the ridges in the two palm images correspond. Ridge-based matching uses ridge pattern landmark features such as sweat pores, spatial attributes, and geometric characteristics of the ridges, and/or local texture analysis, all of which are alternates to minutiae characteristic extraction. This method is a faster method of matching and overcomes some of the difficulties associated with extracting minutiae from poor quality images.

The advantages and disadvantages of each approach vary based on the algorithm used and the sensor implemented. Minutiae-based matching typically attains higher recognition accuracy, although it performs poorly with low quality images and does not take advantage of textural or visual features of the palm. Processing using minutiae-based techniques may also be time consuming because of the time associated with minutiae extraction. Correlation-based matching is often quicker to process but is less tolerant to elastic, rotational, and translational variances and noise within the image. Some ridge-based matching characteristics are unstable or require a high-resolution sensor to

obtain quality images. The distinctiveness of the ridge-based characteristics is significantly lower than the minutiae characteristics.

United States Government Evaluations

Unlike several other biometrics, a large-scale Government-sponsored evaluation has not been performed for palm recognition. The amount of data currently available for test purposes has hindered the ability for not only the Federal Government but also the vendors in efficiently testing and benchmarking commercial palm systems. The FBI Laboratory is currently encoding its hard-copy palm records into three of the most popular commercial palm recognition systems. This activity, along with other parallel activities needed for establishing a National Palm Print Service, will address these limitations and potentially provide benchmark data for US Government evaluations of palm systems.

Standards Overview

Just as with fingerprints, standards development is an essential element in palm recognition because of the vast variety of algorithms and sensors available on the market. Interoperability is a crucial aspect of product implementation, meaning that images obtained by one device must be capable of being interpreted by a computer using another device. Major standards efforts for palm prints currently underway are the revision to the ANSI NIST ITL-2000 Type-15 record. Many, if not all, commercial palm AFIS systems comply with the ANSI NIST ITL-2000 Type-15 record for storing palm print data. Several recommendations to enhance the record type are currently being “vetted” through workshops facilitated by the National Institute for Standards and Technology. Specifically, enhancements to allow the proper encoding and storage of Major Case Prints, essentially any and all friction ridge data located on the hand, are being endorsed to support the National Palm Print Service initiative of NGI.

Summary

Even though total error rates are decreasing when comparing live scan enrollment data with live-scan verification data, improvements in matches between live-scan and latent print data are still needed. Data indicates that fully integrated palm print and fingerprint multi-biometric systems are widely used for identification and verification of criminal subjects as well as in security access applications. But there are still significant challenges in balancing accuracy with system cost. Image matching accuracy may be improved by building and using larger databases and by employing more processing power, but then purchase and maintenance costs will most certainly rise as the systems become larger and more sophisticated. Future challenges require balancing the need for more processing power with more improvements in algorithm technology to produce systems that are affordable to all levels of law enforcement.

Document References

[4] Joe Bonino, Advisory Policy Board Joint Working Group Meeting. 24 April 2002

[1] Peter Komarinski, "Automated Fingerprint Identification Systems": (any publisher info?) 29.

[2] "NEC Solutions America Customer Honored By California's Center for Digital Government," NEC Press Release, December 16, 2004 <http://www.necus.com/companies/20/NECSAMCustomerAwardByCalifCenterDigitalGovt.pdf#search='first%20automated%20palm%20system>.

[3] "Cogent Systems has just received a contract to provide an Advanced Integrated Cogent Automated Palm and Fingerprint Identification System (CAPFIS) for the States of Connecticut and Rhode Island," Cogent Systems Press Release <http://cogt.client.shareholder.com/ReleaseDetail.cfm?ReleaseID=145765>.

[4] CrimTrak, "Fingerprints," Commonwealth of Australia, 2005.

[5] Joe Bonino, Advisory Policy Board Joint Working Group Meeting. 24 April 2002

[6] Shaila K. Dewan, "Elementary, Watson: Scan a Palm, Find a Clue," The New York Times, 21 November 2003.

Speaker Recognition

Introduction

Speaker, or voice, recognition is a biometric modality that uses an individual's voice for recognition purposes. (It is a different technology than "speech recognition", which recognizes words as they are articulated, which is not a biometric.) The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual.

A popular choice for remote authentication due to the availability of devices for collecting speech samples (e.g., telephone network and computer microphones) and its ease of integration, speaker recognition is different from some other biometric methods in that speech samples are captured dynamically or over a period of time, such as a few seconds. Analysis occurs on a model in which changes over time are monitored, which is similar to other behavioral biometrics such as dynamic signature, gait, and keystroke recognition.

History

Speaker verification has co-evolved with the technologies of speech recognition and speech synthesis because of the similar characteristics and challenges associated with each. In 1960, Gunnar Fant, a Swedish professor, published a model describing the physiological components of acoustic speech production, based on the analysis of x-rays of individuals making specified phonic sounds.[1] In 1970, Dr. Joseph Perkell used motion x-rays and included the tongue and jaw[1] to expand upon the Fant model. Original speaker recognition systems used the average output of several analog filters to perform matching, often with the aid of humans "in the loop".[2,3,4,5,6] In 1976, Texas Instruments built a prototype system that was tested by the U.S. Air Force and The MITRE Corporation.[1,7] In the mid 1980s, the National Institute of Standards and Technology (NIST) developed the NIST Speech Group to study and promote the use of speech processing techniques. Since 1996, under funding from the National Security Agency, the NIST Speech Group has hosted yearly evaluations, the NIST Speaker Recognition Evaluation Workshop, to foster the continued advancement of the speaker recognition community.[8]

Approach

The physiological component of voice recognition is related to the physical shape of an individual's vocal tract, which consists of an airway and the soft tissue cavities from which vocal sounds originate.[1] To produce speech, these components work in combination with the physical movement of the jaw, tongue, and larynx and resonances in the nasal passages. The acoustic patterns of speech come from the physical characteristics of the airways. Motion of the mouth and pronunciations are the behavioral components of this biometric.

There are two forms of speaker recognition: text dependent (constrained mode) and text independent (unconstrained mode). In a system using "text dependent" speech, the individual presents either a fixed (password) or prompted ("Please say the numbers '33-54-63'") phrase that is programmed into the system and can improve performance especially with cooperative users. A "text independent" system has no advance knowledge of the presenter's phrasing and is much more flexible in situations where the individual submitting the sample may be unaware of the collection or unwilling to cooperate, which presents a more difficult challenge.[9]

Speech samples are waveforms with time on the horizontal axis and loudness on the vertical access. The speaker recognition system analyzes the frequency content of the speech and compares characteristics such as the quality, duration, intensity dynamics, and pitch of the signal.[1]

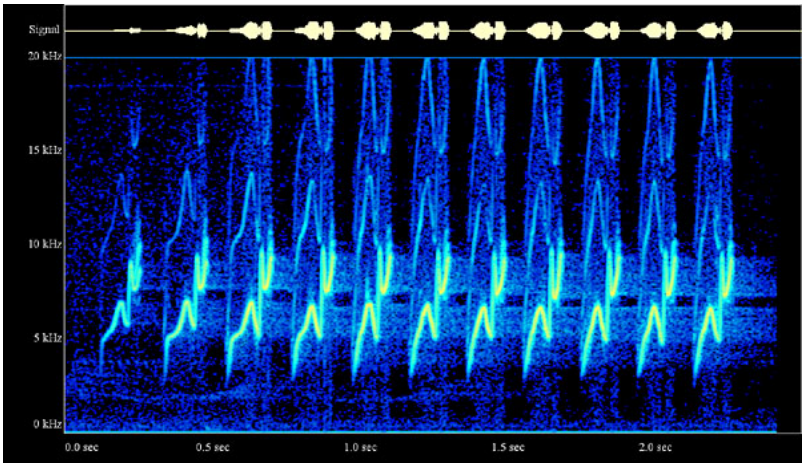


Figure 1: Voice Sample: The voice input signal (top of image) shows the input loudness with respect to the time domain. The lower image (blue) depicts the spectral information of the voice signal. This information is plotted by displaying the time versus the frequency variations.[10]

In "text dependent" systems, during the collection or enrollment phase, the individual says a short word or phrase (utterance), typically captured using a microphone that can be as simple as a telephone. The voice sample is converted from an analog format to a digital format, the features of the individual's voice are extracted, and then a model is created. Most "text dependent" speaker verification systems use the concept of Hidden Markov Models (HMMs), random based models that provide a statistical representation of the sounds produced by the individual. The HMM represents the underlying variations and temporal changes over time found in the speech states using the quality/duration/intensity dynamics/pitch characteristics mentioned above.[9] Another method is the Gaussian Mixture Model, a state-mapping model closely related to HMM, that is often used for unconstrained "text independent" applications. Like HMM, this method uses the voice to create a number of vector "states" representing the various sound forms, which are characteristic of the physiology and behavior of the individual.[1] These methods all compare the similarities and differences between the input voice and the stored voice "states" to produce a recognition decision.

After enrollment, during the recognition phase, the same quality/duration/loudness/pitch features are extracted from the submitted sample and compared to the model of the claimed or hypothesized identity and to models from other speakers. The other-speaker (or "anti-speaker") models contain the "states" of a variety of individuals, not including that of the claimed or hypothesized identity.[9] The input voice sample and enrolled models are compared to produce a "likelihood ratio," indicating the likelihood that the input sample came from the claimed or hypothesized speaker. If the voice input belongs to the identity claimed or hypothesized, the score will reflect the sample to be more similar to the claimed or hypothesized identity's model than to the "anti-speaker" model.[9]

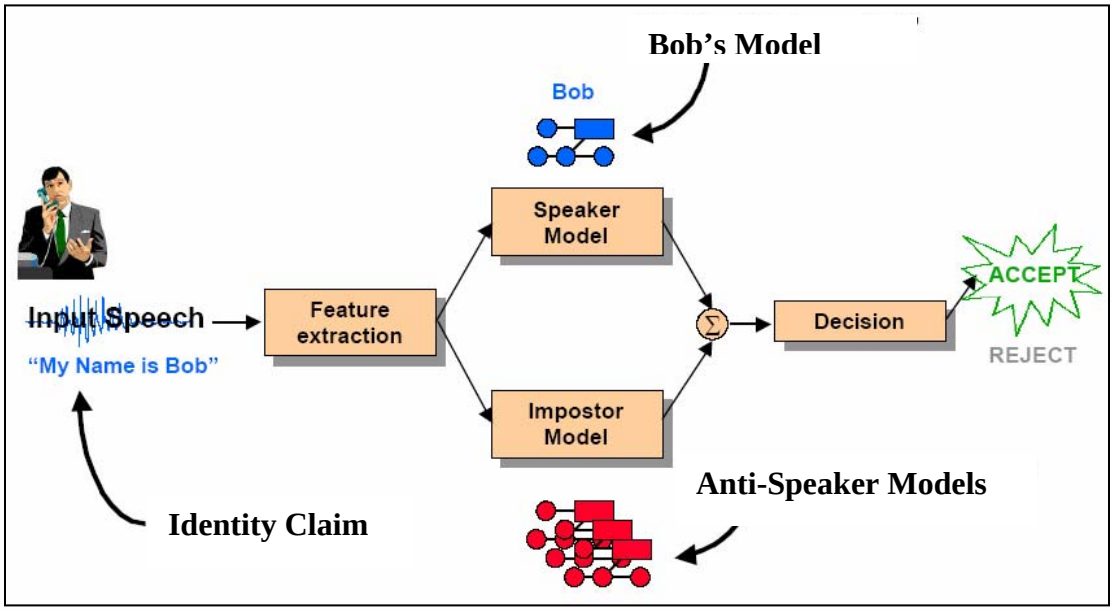


Figure 2: Speaker Verification.[11]

The seemingly easy implementation of speaker recognition systems contributes to their process's major weakness — susceptibility to transmission channel and microphone variability and noise. Systems can face problems when end users have enrolled on a clean landline phone and attempt verification using a noisy cellular phone. The inability to control the factors affecting the input system can significantly decrease performance. Speaker verification systems, except those using prompted phrases, are also susceptible to spoofing attacks through the use of recorded voice. Anti-spoofing measures that require the utterance of a specified and random word or phrase are being implemented to combat this weakness. For example, a system may request a randomly generated phrase, such as "33-54-63," to prevent an attack from a pre-recorded voice sample. The user cannot anticipate the random sample that will be required and therefore cannot successfully attempt a "playback" spoofing attack on the system.

Current research in the area of "text independent" speaker recognition is mainly focused on moving beyond the low-level spectral analysis previously discussed.[9] Although the spectral level of information is still the driving force behind the recognitions, fusing higher level characteristics with the low level spectral information is becoming a popular laboratory technique.[9] (Examples of higher level characteristics include: prosodic

characteristics such as rhythm, speed, modulation and intonation, based on personality type and parental influence; and semantics, idiolects, pronunciations and idiosyncrasies, related to birthplace, socio-economic status, and education level.) Higher level characteristics can be combined with the underlying low-level spectral information to improve the performance of "text independent" speaker recognition systems.

United States Government Evaluations

Since 1996, the National Institute of Standards and Technology (NIST) has been conducting an ongoing series of yearly evaluations called the NIST Speaker Recognition Evaluations (http://www.nist.gov/speech/tests/spk/index.htm), which serve as test beds to compare and collaborate on research efforts across the community. The purpose of the evaluations is to determine the current state of the art, to cultivate technology growth, and to identify the most dominant and promising algorithmic approach to the problems facing speaker recognition.[8]

Standards Overview

Standards play an important role in the development and sustainability of technology, and work in the international and national standards arena will facilitate the improvement of biometrics. The major standards work in the area of speaker recognition involves the Speaker Verification Application Program Interface (SVAPI), which is used by technology developers and allows for compatibility and interoperability between various vendors and networks.

Standards, such as INCITS 398-2005 Common Biometric Exchange Formats Framework (CBEFF), deal specifically with the data elements used to describe the biometric data in a common way, but may not yet apply to speaker recognition techniques.

Summary

Thanks to the commitment of researchers and the support of NSA and NIST, speaker recognition will continue to evolve as communication and computing technology advance. Their determination will help to further develop the technology into a

reliable and consistent means of identification for use in remote recognition.

Document References

[1] John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, Biometrics (New York: McGraw Hill Osborne, 2003).

[2] Potter, Kopp, and Green, Visible Speech (1947).

[3] S. Pruzansky, "Pattern-matching procedure for automatic talker recognition," JASA (26) 1963: 403-406.

[4] K. P. Li, et al, "Experimental studies in SV using an adaptive system," JASA (40) 1966: 966-978.

[5] P. D. Bricker and S. Pruzansky, "Effects of stimulus content and duration on talker identification," JASA (40) 1966: 1441-1449.

[6] K. Stevens, et al, "Speaker authentication and identification: A comparison of spectrographic and auditory presentations of speech material," JASA (44) 1968: 1596-1607.

[7] W. Haberman and A. Fejfar, "Automatic ID of Personnel through Speaker and Signature Verification – System Description and Testing," 1976 Carnahan Conference on Crime Countermeasures, May 1976, University of Kentucky.

[8] "NIST Speaker Recognition Evaluations" 25 April 2005, NIST Speech Group 23 June 2005 <http://www.nist.gov/speech/tests/spk/index.htm>.

[9] Douglas A. Reynolds, "Automated Speaker Recognition: Current Trends and Future Direction," Biometrics Colloquium 17 June 2005.

[10] "Audio Spectrum Analysis," Spectrogram Version 11: A Product of Visualization Software LLC by Richard Horne <http://www.visualizationsoftware.com/gram.html>.

[11] Douglas A. Reynolds (M.I.T. Lincoln Laboratory) and Larry P. Heck (Nuance Communications), "Automatic Speaker Recognition: Recent Progress, Current Applications and Future Trends" 19 February 2000 Presented at the AAAS 2000 Meeting: Humans, Computers and Speech Symposium 19 February 2000 <http://www.ll.mit.edu/IST/pubs/aaas00-dar-pres.pdf>.

Vascular Pattern Recognition

Introduction

Vascular Pattern Recognition, also commonly referred to as Vein Pattern Authentication, is a fairly new biometric in terms of installed systems. Using near-infrared light, reflected or transmitted images of blood vessels of a hand or finger are derived and used for personal recognition. Different vendors use different parts of the hand, palms, or fingers, but rely on a similar methodology. Researchers have determined that the vascular pattern of the human body is unique to a specific individual and does not change as people age. Claims for the technology include that it:

- **is difficult to forge** — Vascular patterns are difficult to recreate because they are inside the hand and, for some approaches, blood needs to flow to register an image.
- **is contact-less** — Users do not touch the sensing surface, which addresses hygiene concerns and improves user acceptance.
- **has many and varied uses** — It is deployed in ATMs, hospitals, and universities in Japan. Applications include ID verification, high security physical access control, high security network data access, and POS access control.
- **is capable of 1:1 and 1:many matching** — Users' vascular patterns are matched against personalized ID cards/smart cards or against a database of many scanned vascular patterns.

History

Potential for the use of this technology can be traced to a paper prepared in 1992 by Dr. K. Shimizu[1], in which he discussed optical trans-body imaging and potential optical CT scanning applications. In 1996, author Yamamoto K[2], in conjunction with K. Shimizu, presented another paper in which the two discussed research they had undertaken since the earlier paper.

The first research paper about the use of vascular patterns for biometric recognition was published in 2000.[3] This paper describes the technology that uses the subcutaneous blood vessel pattern in the back of the hands and that was to become the first

commercially available vascular pattern recognition system in 2000. Additional research has further improved the technology.[4,5,6] The introduction of this technology inspired additional research and commercialization into finger- and palm-based systems.[7,8]

Approach

Vascular pattern in the back of hands

Near-infrared rays generated from a bank of light emitting diodes (LEDs) penetrate the skin of the back of the hand. Due to the difference in absorbance of blood vessels and other tissues, the reflected near-infrared rays produce an image on the sensor. The image is digitized and further processed by image processing techniques producing the extracted vascular pattern. From the extracted vascular pattern, various feature data such as vessel branching points, vessel thickness, and branching angles are extracted and stored as the template.

Vascular pattern in fingers

The basic principle of this technology is shown in Figures 1 & 2. Near-infrared rays generated from a bank of LEDs penetrate the finger or hand and are absorbed by the hemoglobin in the blood. The areas in which the rays are absorbed (i.e., veins) appear as dark areas similar to a shadow in an image taken by a Charge-Coupled Device (CCD) camera. Image processing can then construct a vein pattern from the captured image. Next this pattern is digitized and compressed so that it can be registered as a template.

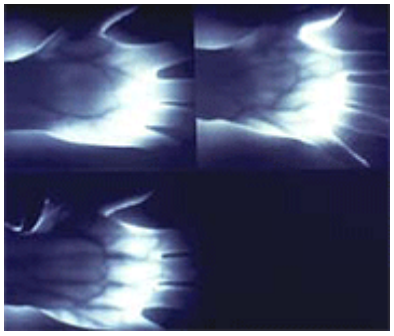


Figure 1. Transmittance Images of a Hand.[9]

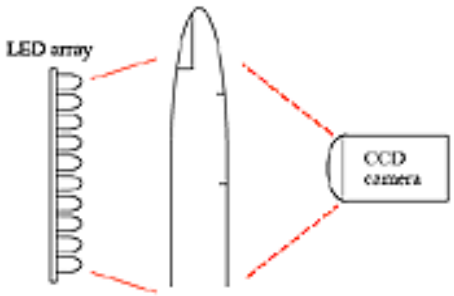


Figure 2. Principle of Transmittance Imaging.[9]

United States Government Evaluations

The US Government has not performed technology evaluations of vascular pattern recognition biometrics at this time.

Summary

Vascular pattern recognition has gained sponsorship from companies that have developed reputations for developing products that compete successfully in global markets. There appears to be some testing and validation by third parties. Standards work will need to be accomplished before this technology can grow to broader acceptance.

Document References

[1] K. Shimizu, "Optical trans-body imaging – Feasibility of optical CT and Functional Imaging of Living Body," Medicina Philosophica, 11:620-629, 1992.

[2] K. Shimizu and K. Yamomoto,"Imaging of Physiological Functions By Laser Transillumination," OSA TOPS on Advances Optical Imaging and Photom Migration, 2:348-352, 1996.

[3] Sang-Kyun Im, Hyung-Man Park, Young-Woo Kim, Sang-Chan Han, Soo-Won Kim, and Chul-Hee Kang, "Biometric Identification System by Extracting Hand Vein Patterns," Journal of the Korean Physical Society, Vol. 38, No. 3, March 2001: 268-272.

[4]Sang-Kyun Im, Hwansoo Choi, and Suwon Kim, "Design for an Application Specific Processor to Implement a Filter Bank Algorithm for Hand Vascular Pattern Verification," J. of Korean Physics Society, 2002, Vol. 41: 461-467.

[5]Sang-Kyun Im and Hwansoo Choi, "A Filter Bank Algorithm for Hand Vascular Pattern Biometrics," Proceedings of ICCARV'02, 2002: 776-781.

[6]Sang-Kyun Im, Hwansoo Choi, and Suwon Kim, "A Direction-based Vascular Pattern Extraction Algorithm for Hand Vascular Pattern Verification," ETRI J., Vol. 25-2, 2003: 101-108.

[7] Y. Taka, Y. Kato, and K. Shimizu, "Transillumination Imaging of Physiological Functions by NIR Light," World Congress on Medical Physics and Biomedical Engineering 2000, CD-ROM, 4982-14105.

[8] "New Biometric Technologies Get Beneath the Surface," IDNewswire, 14 October 2005, Vol. 4, No. 18, <http://www.cardtechnology.com/article.html?id=20051026CTDMQSN1>.

[9] Xin Wang, Kozo Sushita and Koichi Shimizu, "Our Breakthrough Technology" <http://www.iaccess-systems.com/bloodvessel.htm>.

Biometrics Standards

Introduction

Standards for the collection, storage, and sharing of biometric data are of utmost importance to government and private systems. This paper provides an entry-level understanding of how biometric standards are developed and the current status of biometric standards by answering the following questions:

- What are biometric standards?
- Why are biometric standards important?
- What types of biometric standards are there?
- Who develops standards?
- How are standards developed?
- What is conformity assessment?
- Is the use of biometric standards mandatory or optional?
- Where do I find more information about a specific standard?

What are biometric standards?

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Guide 2:2004 defines a standard as "a document, established by consensus that provides rules, guidelines or characteristics for activities or their results." [1] The Biometric Consortium website defines standards as "a general set of rules to which all complying procedures, products or research must adhere." [2]

Standards play a role in everyday life by establishing the size, configuration, or protocol of a product, process, or system. Standards specify performance of products or personnel and also define terms so that there is no misunderstanding among those using the standards.

As examples, standards help ensure that film to fit 35mm cameras can be purchased anywhere in the world, that a light bulb fits a socket, and that plugs for electrical appliances fit outlets. With design and performance standards, homes, workplaces and public buildings are safer from collapse, fire and explosion.[3]

For any given technology, standards assure the availability of multiple sources for comparable products and of competitively-

priced products in the marketplace. Standards support the expansion of the marketplace.[4]

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. As a process, a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.[5]

Biometric standards specify:

- formats for the interchange of biometric data;
- common file formats that provide platform independence and separation of transfer syntax from content definition;
- application program interfaces and application profiles;
- performance metric definitions and calculations;
- approaches to test performance; and
- requirements for reporting the results of performance tests.

Why are biometric standards important?

Standards enable development of integrated, scalable, and robust solutions and reduce the cost of development and maintenance of system solutions. Biometric standards have been and are currently being developed on both the national and international levels. These efforts are focusing on creating a standard set of biometric data interchange definitions, developing standards to promote interoperability between various systems, and creating standards for testing biometrics and for testing conformance to biometric standards. Standards should be technology neutral and not favor any particular vendor or modality.[5]

What types of biometric standards are there?

Biometric standards include, but are not limited to:[6]

- Technical Interfaces — specify interfaces and interactions between biometric components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems; and specify the architecture and operation of biometric systems in order to identify the standards that are needed to support multi-vendor systems and their applications. Examples include ANSI INCITS 358-2002 BioAPI Specification v1.1 and ANSI INCITS 398-2005 [NISTIR 6529-A] Common Biometric Exchange File Format (CBEFF).
- Data Interchange Formats — specify the content, meaning, and representation of formats for the interchange of biometric data, e.g., Finger Pattern Based Interchange Format, Finger Minutiae Format for Data Interchange, Face Recognition Format for Data Interchange, Iris Interchange Format, Finger Image Based Interchange Format, Signature/Sign Image Based Interchange Format, and Hand Geometry Interchange Format; and specify notation and transfer formats that provide platform independence and separation of transfer syntax from content definition. Examples include ANSI INCITS 377-2004 Finger Pattern Based Interchange Format, ANSI INCITS 378-2004 Finger Minutiae Format for Data Interchange, and ANSI INCITS 379-2004 Iris Image Interchange Format.
- Application Profile Standards — specify one or more base standards and standardized profiles, and where applicable, the identification of chosen classes, conforming subsets, options, and parameters of those base standards or standardized profiles necessary to accomplish a particular function. Examples include ANSI INCITS 383-2003 Biometrics-Based Verification and Identification of Transportation Workers, and ANSI INCITS 394-2004 Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management.
- Performance Testing and Reporting — specify biometric performance metric definitions and calculations, approaches to test performance, and requirements for

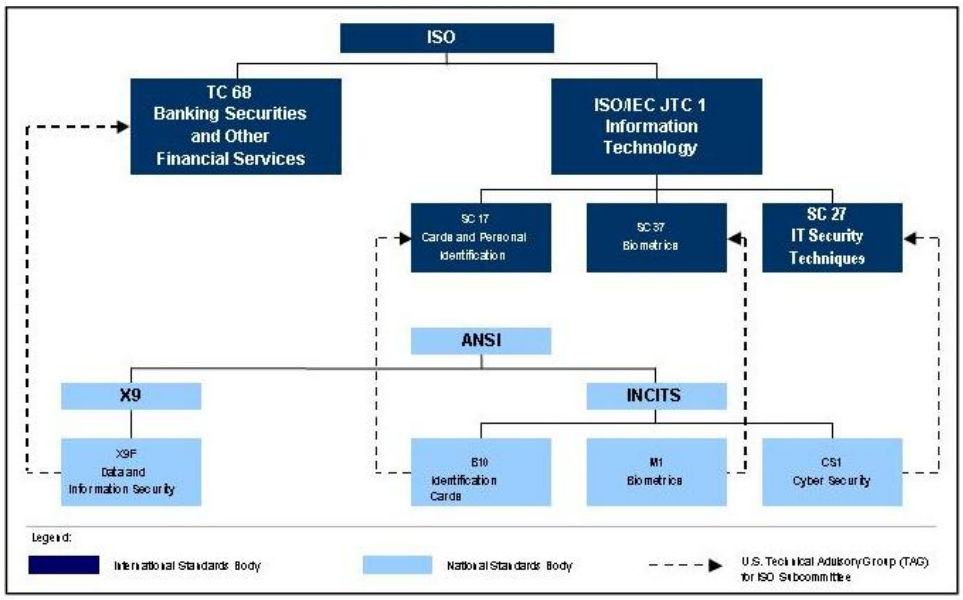
reporting the results of these tests. Examples include ANSI INCITS 409.1-2005 Biometric Performance Testing and Reporting Part 1 - Principles Framework; ANSI INCITS 409.2-2005 Biometric Performance Testing and Reporting Part 2 - Technology Testing Methodology; and ANSI INCITS 409.3-2005 Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies.

Who develops standards?

A few of the better known Standards Development Organizations (SDOs) and government agencies who support standards development in biometrics include:

- InterNational Committee for Information Technology Standards (INCITS) M1
- National Institute of Standards and Technology
- Joint Technical Committee 1 (JTC 1)/Subcommittee 37 (SC 37)
- Organization for the Advancement of Structured Information Standards (OASIS)

Each of the following subsections provides a brief description of each SDO.



INCITS M1

INCITS is accredited by and operates under rules approved by the American National Standards Institute (ANSI). INCITS is the primary US focus of standardization in the field of Information and Communications Technologies (ICT), encompassing storage, processing, transfer, display, management, organization, and retrieval of information. INCITS also serves as ANSI's Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1 (JTC 1), which is responsible for international standardization in the field of Information Technology.

In November 2001, INCITS established M1 with membership open to any organization (e.g., academic institutions, federal agencies, companies) directly and materially affected by M1 activities. As the US TAG to SC 37, INCITS M1 is responsible for establishing US positions and contributions to SC 37, as well as representing the US at SC 37 meetings. M1 presently has five standing task groups:

- M1.2 Biometric Technical Interfaces — develops standards for interfaces and interactions between biometric system components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems.
- M1.3 Biometric Data Interchange Formats — develops standards for the content, meaning, and representation of biometric data interchange formats.
- M1.4 Biometric Profiles — develops profile standards to ensure the interoperability of biometric information in specific applications (e.g., Biometric Based Verification and Identification of Transportation Workers, Border Management, Point of Sale).
- M1.5 Biometric Performance Testing and Reporting — develops standards for biometric performance metric definitions and calculations, and approaches to test performance and requirements for reporting the results of these tests.
- M1.6 Societal Aspects of Biometric Implementations — develops technical reports that address the study and standardization of technical solutions to cross-jurisdictional and societal aspects of biometric implementations.

In addition to the standing task groups, M1 has the ability to form Ad Hoc Groups to perform a specific task and report back to the

parent body, e.g. M1 or M1.3. Upon completion of its report, or at the second meeting of the parent body following the Ad Hoc Group's establishment, the Ad Hoc Group is dissolved unless there is sufficient reason to extend its duration. Examples include the Ad Hoc Group on Data Quality (QUAHOG), the Ad Hoc Group on the Use of BioAPI to Support Ten-print Capture (AHGUBSTC), the Ad Hoc Group on Round Robin Testing (AHGRRT), and the Ad Hoc Group on INCITS 378 Encoding Rules (AHGIER). Since an Ad Hoc Group is limited in duration and scope, its business may be conducted less formally than that of any other INCITS Organizational Entity (IOE), so the documentation of its report serves as principal record of the group.

National Institute of Standards and Technology (NIST)

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by NIST for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use Government-wide. In addition to being the nation's premier measurement research laboratory, NIST develops FIPS when there are compelling Federal Government requirements such as for security and interoperability for which no acceptable industry standards or solutions exist. FIPS do not apply to national security systems. Other documents published by NIST include NIST Interagency Reports (NISTIR) and NIST Special Publications. Examples of these are NISTIR 6529-A, "Common Biometric Exchange Formats Framework (CBEFF) " and NIST Special Publication SP 500-245, "ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information," respectively.

JTC 1/SC 37

JTC 1/SC 37 is responsible for the international standardization projects for generic biometric technologies to support data interchange, interoperability, and testing. Established in June 2002 by JTC 1, SC 37 has twenty-one participating member countries, six observer countries, and eleven liaison organizations. As with INCITS M1, SC 37 has maintained fast-paced development activities since its inception, due to the increased demand for proven biometric technologies. To manage these efforts, SC 37 has also organized a number of Working Groups (WGs) that closely align with the M1 Task Groups:

- WG1 Harmonized Biometric Vocabulary — develops standardized definitions for biometric vocabulary terms.

- WG2 Biometric Technical Interfaces — develops international standards for BioAPI and CBEFF, as well as a number of other related projects.
- WG3 Biometric Data Interchange Formats — develops international versions of the biometric data interchange format standards.
- WG4 Biometric Functional Architecture and Related Profiles — develops international biometric profile standards to support biometric interoperability for applications.
- WG5 Biometric Testing and Reporting — develops international standards for biometric performance testing and reporting.
- WG6 Cross-jurisdictional and Societal Aspects — currently developing an international technical report on privacy concerns and other social concerns related to biometric standards.

OASIS

OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces Web services standards along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.[7]

OASIS XML Common Biometric Format (XCBF) provides a standard way to describe information that verifies identity based on human characteristics such as DNA, fingerprints, iris scans, and hand geometry. The OASIS XCBF Technical Committee defined a common set of secure XML encodings for the patron formats specified in the Common Biometric Exchange File Format (CBEFF) (NISTIR 6529). These XML encodings are based on the ASN.1 schema defined in ANSI X9.84:2003 Biometrics Information Management and Security. They conform to the XML Encoding Rules (XER) for ASN.1 defined in ITU-T Recommendation X.693, and rely on the security and processing requirements specified in X9.96 XML Cryptographic Message Syntax (XCMS).[7]

Security Assertion Markup Language (SAML), developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows

business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.[7]

How are standards developed?

Consensus standards are commonly developed using a process that proceeds from a project proposal to the cyclic writing, editing, and commenting of the Draft Standard, which, upon approval by the member bodies, culminates in the Published Standard. The following outlines one such possible process:

- Project Proposal
- Draft Standard
  - Working Draft
  - Committee Draft
  - Final Draft
- Member Body Approval
- Published Standard

Successive drafts may be considered until consensus is reached on the technical content. Once consensus has been attained, the text is circulated to all member bodies for voting and comments within a period set by the SDO. If the approval criteria, which vary from SDO to SDO and can range from a simple majority of members voting to other more complex criteria, are not met, the Draft Standard is returned for further study and a revised Draft Standard will again be circulated for voting and comments. Most SDOs review their standards at specified time intervals, to determine whether a given standard should be confirmed, revised, or withdrawn.

If a document with a certain degree of maturity is available at the start of a standardization project, for example a standard developed by another organization, it is possible to omit certain stages of the process. In a so-called “fast-track procedure,” a document is submitted directly to the member bodies for approval as a draft standard without passing through the previous stages.[8]

What is conformity assessment?

ISO/IEC Guide 2:1996 defines conformity assessment as "any activity concerned with determining directly or indirectly that relevant requirements are fulfilled".[3] Conformity assessment of a product to a given standard raises the user's assurance that the product will perform in the manner expected with regard to the intent of the written specification.

While a standard is a technical expression of how to make a product safe, efficient, and compatible with others, a standard alone cannot guarantee performance. Conformity assessment, however, provides assurance to users by increasing consumer confidence when personnel, products, systems, processes, or services are evaluated against the requirements of a standard.[3]

The development of conformance tools makes possible the establishment of conformity assessment programs to validate conformance, e.g., to ANSI INCITS 358-2002 BioAPI Specification v1.1, and to support development of products conforming to voluntary consensus biometric standards. By making the tools available, developers may use these same test tools to ensure standards conformance before products are released.

Is the use of biometric standards mandatory?

In general, standards usage is optional. However, the real benefits of standards are realized by organizations that require the application and use of standards. Some organizations maintain a registry or database of standards that must be applied in acquiring, developing, and maintaining systems. These organizations will not purchase products or services that do not conform to such required standards.

Where do I find more information about a specific standard?

An excellent starting point for more information about a specific standard is the websites of organizations that help develop the standard, e.g., http://www.iso.org, http://www.ansi.org, http://www.nist.gov, etc. There are also additional online resources available such as NSSN: A National Resource for Global Standards (http://www.nssn.org/search.html) and the World

Standards Services Network (http://www.wssn.net/WSSN/index.html).

Document References

[1] ISO/IEC Guide 2:2004 <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39976&ICS1=1&ICS2=120&ICS3=>.

[2] The Biometric Consortium, "Standards Activities," <http://www.biometrics.org/html/standards.html>.

[3] American National Standards Institute, "Frequently Asked Questions," <http://www.ansi.org/about_ansi/faqs/faqs.aspx?menuid=1>.

[4] National Institute of Standards and Technology – Information Technology Laboratory, "Biometrics Standards and Current Standard-Related Activities" 18 February 2002 (updated 8 January 2003) <http://www.itl.nist.gov/div893/biometrics/standards.html>.

[5] National Science & Technology Council Subcommittee on Biometrics, "Frequently Asked Questions" 16 August 2005 <http://www.biometricscatalog.org/biometrics/FAQDec2005.pdf> .

[6] InterNational Committee for Information Technology Standards, "M1 - Biometrics" <http://www.ncits.org/tc_home/m1.htm>.

[7] Organization for the Advancement of Structured Information Standards <http://www.oasis-open.org/>.

[8] International Organization for Standardization, "Stages of the development of International Standards" 30 September 2003 <http://www.iso.org/iso/en/stdsdevelopment/whowhenhow/proc/proc.html>.

Standards Glossary

AHGIER	Ad Hoc Group on INCITS 378 Encoding Rules
AHGRRT	Ad Hoc Group on Round Robin Testing
AHGUBSTC	Ad Hoc Group on the Use of BioAPI to Support Ten-print Capture
ANSI	American National Standards Institute
CBEFF	Common Biometric Exchange File Format

FIPS	Federal Information Processing Standards
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
IOE	INCITS Organizational Entity
ISO	International Organization for Standardization
JTC 1/SC 37	Joint Technical Committee 1/Subcommittee 37
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Reports
OASIS	Organization for the Advancement of Structured Information Standards
QUAHOG	Ad Hoc Group on Data Quality
SAML	Security Assertion Markup Language
SDO	Standards Development Organizations
SMT	Scar Mark & Tattoo
TAG	Technical Advisory Group
WG	Working Group
XCBF	XML Common Biometric Format
XCMS	XML Cryptographic Message Syntax
XER	XML Encoding Rules

Introduction

Determining the best biometric system for a specific operational environment and how to set up that system for optimal performance requires an understanding of the evaluation methodologies and statistics used in the biometrics community. This document provides a baseline testing and statistics review, thus enabling appropriate analysis of available research reports. This document is intended to further the understanding of a general audience and is not intended to replace or compete with sources that may be more technically descriptive/prescriptive such as those under development by standards bodies such as INCITS and ISO/IED. Detailed information on how to properly perform performance evaluations is beyond the scope of this document.

Evaluation Types

Performance evaluations of biometric identification technology are divided into three overlapping categories with increasing complexity in uncontrolled variables: technology, scenario, and operational.[1] A thorough evaluation of a system for a specific purpose starts with a Technology Evaluation, followed by a Scenario Evaluation, and finally an Operational Evaluation.

The primary goal of Technology Evaluations is to measure the performance of biometric systems, typically only the recognition algorithm component. They are repeatable and usually short in duration. Technology Evaluations are usually performed using standard datasets collected previous to testing. In general, results from a Technology Evaluation show specific areas that require future research and development (R&D) and provide performance data that is useful when selecting algorithms for scenario evaluations. An example of a Technology Evaluation is the Face Recognition Vendor Test.[2]

The primary aim of Scenario Evaluations is to measure performance of a biometric system operating in a particular application. For example, testing biometrics for access control purposes at a mock doorway in a laboratory. Each tested system normally would have its own acquisition sensor and would thus receive and produce slightly different data. For this and other reasons, Scenario Evaluations are not always completely

repeatable. Scenario Evaluations usually take a few weeks to complete because multiple trials (and for some Scenario Evaluations, multiple trials of multiple subjects/areas) must be completed to ensure adequate habituation of the end users (if the scenario calls for it) and to achieve a statistically relevant number of samples. Results from a typical Scenario Evaluation show areas that require additional system integration and provide performance data on systems for the application tested. An example of a Scenario Evaluation is the UK Biometric Product Testing.[3]

At first glance, an Operational Evaluation appears very similar to a Scenario Evaluation, except that the test is conducted at the actual site using actual end users, a subset of the end users, or a representative set of subjects. Rather than testing for performance (which is difficult, if not impossible, to do in some operational evaluations), Operational Evaluations typically aim to determine the workflow impact caused by the addition of a biometric system. Operational Evaluations are typically not repeatable. Operational Evaluations can last from several weeks to several months because the evaluation team must first examine workflow performance prior use of the technology and again after users are familiar with the technology. An accurate analysis of the benefit of the new technology requires a comparison of the workflow performance before and after use of the technology.

In an ideal three-step evaluation process, Technology Evaluations are first performed on all applicable technologies that could conceivably meet requirements. The technical community then uses the results to plan future R&D activities, while potential users use the results to select promising systems for application-specific Scenario Evaluations. Results from the Scenario Evaluation(s) will enable users to determine the best system for their specific application and to have a good understanding of how it will operate at the proposed location. This performance data, combined with workflow impact data from subsequent Operational Evaluations, will enable decision makers to develop a solid business case for potential installations.

So for those analyzing evaluation reports, it is important to determine which type of evaluation occurred and its relevance to an intended application. Generally, technology evaluation reports contain information relevant to most intended applications of a given biometric, while operational evaluation reports are generally only useful if the intended application is very closely related to what was tested.

Biometric Evaluation Terms

Biometric terms such as recognition, verification and identification are sometimes used interchangeably. This is not only confusing but incorrect as each term has a different meaning.

- Verification occurs when the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates.
- Identification occurs when the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is "closed-set" if the person is assumed to exist in the database. In "open-set" identification, the person is not guaranteed to exist in the database. The system must determine if the person is in the database. A "watchlist" task is an example of "open-set" identification.
- Recognition is a generic term and does not necessarily imply either verification or identification. All biometric systems perform "recognition" to "again know" a person who has been previously enrolled.

This section provides in-depth, clearly defined descriptions of these tasks. To help explain them, a hypothetical face recognition system must be introduced. This hypothetical face recognition system can compare one image to another and provide scores (*similarity scores*[a]) for each comparison. For our example system, the similarity scores range from 0.0 to 1.0, with a 1.0 score being an exact match. The system also has a user-set "threshold" that the system uses to make a matching decision. Although the examples in this section use face recognition, the tasks and associated performance measures are the same as for other biometric types.

[a] Not all biometric systems use similarity scores for comparisons. Some use difference scores, hamming distances, etc. For the purposes of this non-technical paper, the basic concept is essentially the same – mathematically comparing two biometric templates in order to make a matching decision.

Verification

In the verification task, an end user must first make a claim as to his/her identity (e.g., I am John Q. Public) and the biometric system then determines if the end-user's identity claim is true or false. A good example is verifying an end user's identity, frequently represented by a username, by requiring a password prior to providing access to his/her account on a computer system. Figure 1 gives a visual example where the gentleman on the right makes a claim that he is the gentleman on the left. For this example, assume these are pictures of the same individual.

Figure 1: Correct Verification Claim.

Assume that the example face recognition system produces a similarity score of 0.93 for this verification trial. (Remember that our demonstration face recognition system works on a 0.0 to 1.0 scale with 1.0 being an exact match.) Also assume that the system's verification threshold was set at 0.90. Since 0.93 is higher than 0.90, the system in this example has correctly determined that the gentleman in the right picture is the same as the gentleman in the left picture. This is called a true accept or correct verification.

Now assume that the same individual in Figure 1 makes the same claim, except this time the system's verification threshold is set at 0.95. In this case, the demonstration face recognition system will not make a correct decision.[b]

If we run many trials with this gentleman, as well as other correct matches, we will know the rate[c] at which legitimate end users are correctly verified by the system. This is called the true accept or correct verification rate.

[b] This situation is referred to as a *false reject*.
[c] Technically, these tests will produce a statistical estimate of the actual rate. For simplicity sake, the term "rate" is used in this introductory document.

Figure 2 shows a different verification claim. In this example, the gentleman on the right claims to be the gentleman on the left. Obviously, this is not the case. Assume that the system returns a similarity score of 0.86. Let us also assume that the system's verification threshold was set at 0.9. In this example, the face recognition system determines that the gentleman on the right is not the gentleman on the left.

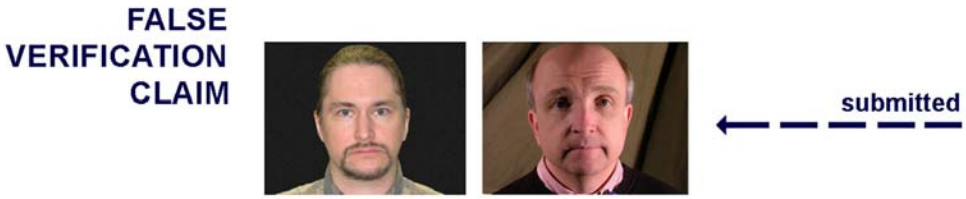


Figure 2: False Verification Claim.

Now let us look at the case where the same individual in Figure 2 makes the same claim, but the system's verification threshold is set at 0.85. In this case, the system incorrectly verifies that the gentleman is the gentleman in the system. This error is called a false accept. If many trials are run with incorrect claims, the rate at which the system incorrectly matches an imposter individual to another individual's existing biometric will be known. This is called the false accept rate.

Ideally, biometric systems would always provide a probability of verification of 100% with a false accept rate of 0%.[d] Unfortunately, that is not possible; so system administrators must compromise by setting the system's threshold at an optimum value for their given application. Determining the threshold can be difficult because the verification rate and false accept rate are not independent variables.[e] If the threshold in the example face recognition system is raised, the verification rate decreases, but the false accept rate also decreases. If the threshold in the example system is lowered, the verification rate rate increases, but the false accept rate also increases. Plotting verification

[d] From a statistical standpoint, neither of these results is even possible. Someone may run a test with no observed errors, but they statistically wouldn't have a 100% reliable system. All documented results should meet basic statistic principles.

[e] This relationship is similar to that of a metal detector. By adjusting the threshold, security personnel increase the chances of it alarming on larger or smaller metal items.

accept rates against the associated false accept rates, called a Receiver Operating Characteristic (ROC) curve, allows for a visualization of this trade-off relationship. Figure 3 is a sample of a verification ROC (with fabricated numbers for example purposes). Varying the system's threshold moves the operating point along its ROC curve.

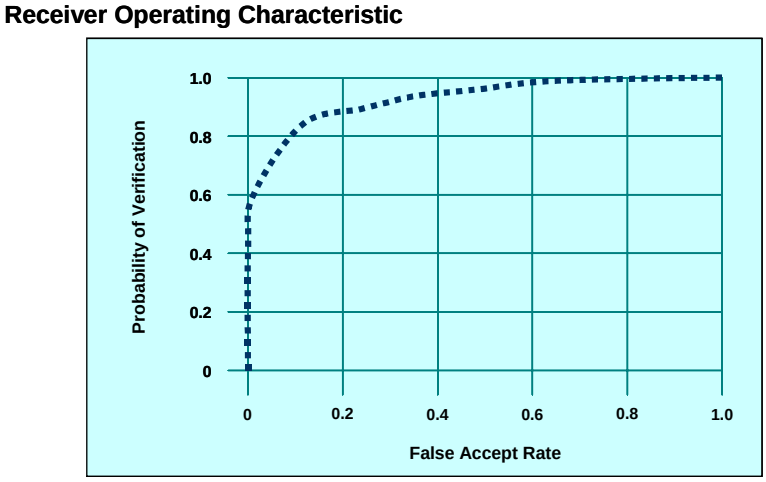


Figure 3: Example Verification ROC.

Open-Set Identification

In open-set identification (sometime referred to as a watchlist application), the biometric system determines if the individual's biometric template matches a biometric template of someone in the database. The individual does not make an identity claim and, in cases of covert identification, does not personally interact with the system whatsoever. Examples of this task might be comparing biometrics of visitors to a building against a terrorist database, or comparing a biometric of a "John Doe" in a hospital to a missing person's database. Figure 4 shows an image of a gentleman as an input to the example face recognition system.

The system first compares the submitted image to each image in the database. Assume that the similarity score for each comparison is 0.6, 0.86, 0.9, and 0.4 (respectively). Also assume that the system's watchlist threshold is set at 0.85. In this example, the face recognition system sounds an alarm each time one or more of the similarity scores is higher than the threshold. Since an alarm sounded, the system user would look more closely at the similarity scores to see which image attained the highest score, which would be the system's best guess at the identity of

the subject in the input image. We can easily see that it is correct. (This description is only concerned with the top match, so the fact that a second comparison also had a similarity score higher than the threshold is irrelevant.) This example produced what is called a *correct detect and identify*.

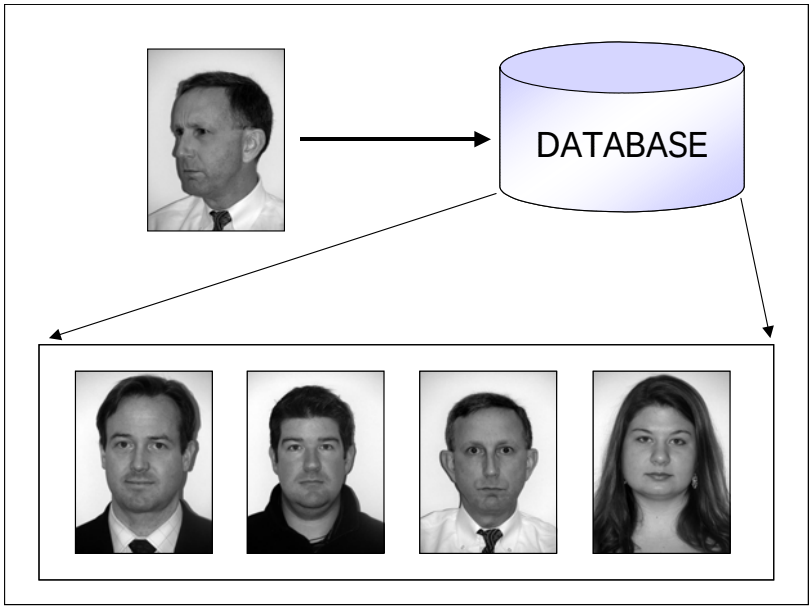


Figure 1: Watchlist Example 1.

Consider again the example shown in Figure 4, except this time the watchlist threshold is 0.95. In this case, the face recognition system does not sound an alarm because none of the similarity scores (0.6, 0.86, 0.9, and 0.4) are above the system's threshold. Since there was no alarm, there would be no reason to look further at the similarity scores. Thus, for this example, the demonstration face recognition system did NOT produce a *correct detect and identify*.

Taking a final look at the example shown in Figure 4, assume that the similarity score for each comparison is 0.6, 0.86, 0.8, and 0.4, respectively, and the watchlist threshold is 0.75. In this example, the system sounds an alarm as one or more of the similarity scores are higher than the threshold. The system user would look more closely at the similarity scores and see that the second individual has the highest score. In this example, an alarm correctly sounded (as the subject is in the database), but the demonstration face recognition system did not correctly choose the identity of the gentleman as the top-ranked match. Thus, the system did NOT produce a *correct detect and identify*.

If we run many trials, we will know how often the system will return a correct result. A correct result occurs when an individual who is in a database causes a system alarm AND is properly identified in an open-set identification (watchlist) application. This is called the *Detect and Identification Rate.*

Now consider an alternative setup where the input does not have a corresponding match in the database, as shown in Figure 5. In this example, an image of a lady is the input to our example face recognition system, which must determine if this individual is in the database.

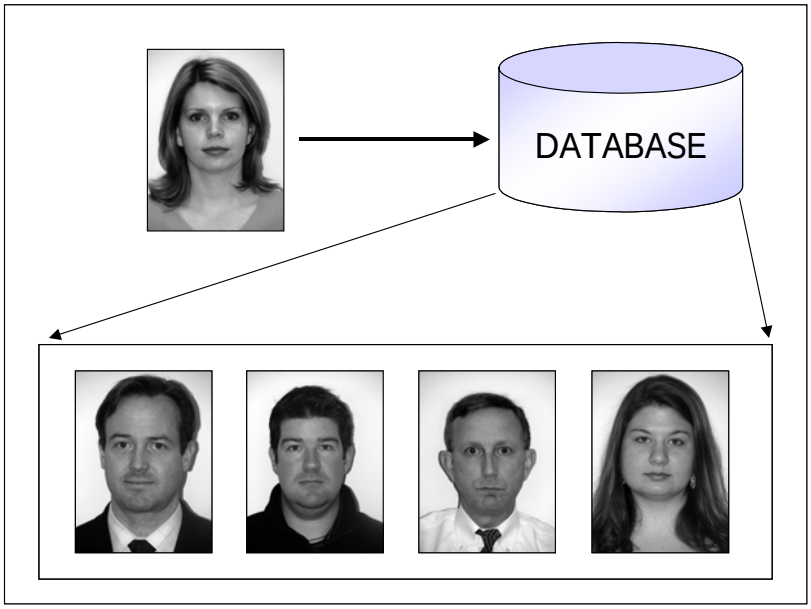


Figure 2: Watchlist Example 2.

The system first compares the input image to each image in the database. Assume that the similarity score for each comparison is 0.7, 0.8, 0.4, and 0.6, respectively, and the system's watchlist threshold is set at 0.85. In this example, an alarm will not sound, as none of the similarity scores are higher than the threshold.

Now consider the same example with a threshold set at 0.75. In this case, an alarm sounds because one of the similarity scores is higher than the threshold. This is an incorrect alarm, because the lady in the input image is not in the database. This is called a *false alarm*. If we run many trials with subjects who are not in the database, we will know how often the system will return an incorrect alarm, i.e., the *false alarm rate*.

Because biometric systems cannot provide a detection and identification rate of 100% with a false alarm rate of 0%, system administrators must set the system's threshold at an optimum value for the given application and the tradeoffs of correctly identifying subjects versus false alarms. If the watchlist threshold in the example system is raised, the identification rate decreases, but the false alarm rate also decreases. If the watchlist threshold is lowered, the identification rate increases, but the false alarm rate increases. Plotting the identification rates and the associated false alarm rates, also called a *Receiver Operating Characteristic* (*ROC),* allows for a visualization of this trade-off relationship. These are sometimes referred to as a Watchlist ROC or an Identification ROC to help differentiate it from a verification ROC. Figure 6 is an example watchlist *ROC* (with fabricated numbers).

Watchlist ROC

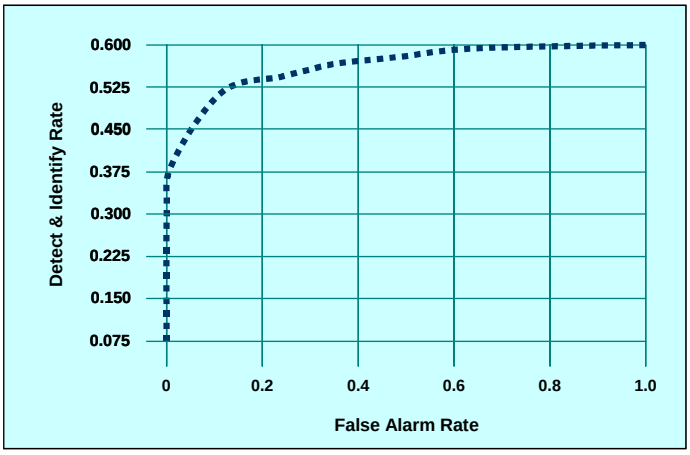


Figure 1: Example Watchlist ROC.

Database size is important to watchlist performance. The Face Recognition Vendor Test (FRVT) 2002[4] showed that watchlist performance for face recognition systems decreases as the size of the database increases. (Effectively, the curve in Figure 6 will lower as the size of the database increases.) When quoting open-set identification performance, it is important to also state the database size.

In practice, the open-set identification task is much more difficult for biometric systems (and presumably for human operators) than the verification task. When discussing a specific application, it is critical to think in terms of the proper task and the associated

statistics. Failure to do so will lead to significant confusion and errors.

Closed-Set Identification

Closed-set identification is where every input image has a corresponding match in the database. In practice, there are very few applications that operate under the closed-set identification task. Even the FBI's Integrated Automated Fingerprint Identification System (IAFIS) operates as a watchlist -- an open-set identification task. However, these statistics are routinely found in research and evaluation reports, as they are a good measure of showing general strengths and weaknesses.

In the closed-set identification task, a biometric template of an individual is presented to the biometric system, as shown in Figure 4. Again, it is known that the person is in the database. The example face recognition system first compares the input image to each image in the database. Let us assume that the similarity score for each comparison is 0.6, 0.86, 0.9, and 0.4, respectively. In this example, the correct match has the top similarity score. If we run the same trial for all subjects in the database, we will know how often the system will return a correct result with the top match, which is termed the identification rate at rank 1.

Still referring to the example shown in Figure 4, assume that the similarity score for each comparison is 0.6, 0.4, 0.8, and 0.86, respectively. In this case, the correct match is the second highest similarity score. If we run the same trial for all subjects in the database, we will know how often the system will return a correct result in either the top or second ranked score. (We do not necessarily care if they are in the top or second rank specifically, just that they are in one of those positions.) This is termed the identification rate at rank 2.

These two examples show a trend for how to show identification performance graphically. The probability of correct identification at rank 20 means, what is the probability that the correct match is somewhere in the top 20 similarity scores? A Cumulative Match Characteristic (CMC) curve shows the probability of identification for numerous ranks. Figure 7 is an example CMC (with fabricated numbers for example purposes).

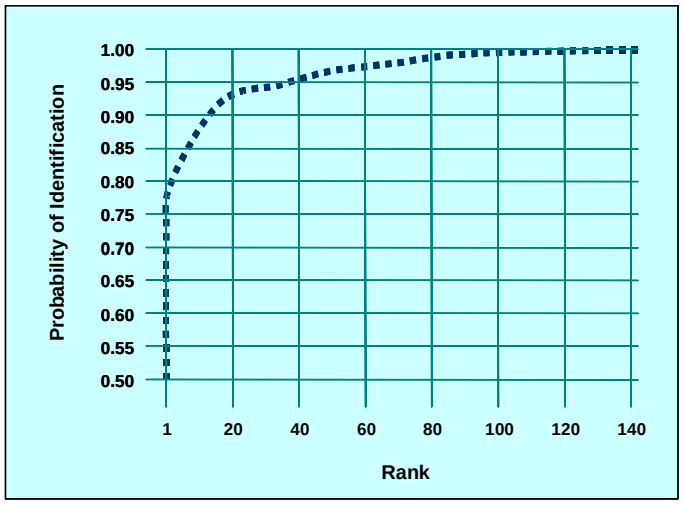


Figure 2: Example Cumulative Match Characteristic Curve.

One key feature of a CMC is that, in a plot that includes all possible ranks (e.g., if the database has 140 people, and the CMC goes through rank 140), the probability of identification is 100% at the highest (140 in this example) rank. This is true because every input is in the database (otherwise this is an open-set identification task instead of a closed-set identification task), and it is showing the identification rate for the entire database.

Just as in the watchlist task, it is important to state the size of the database when describing a CMC curve. The probability of correct identification at rank 10 for a 100-person database would be much better than the probability of correct identification at rank 10 for a 10,000-person database (all other factors being the same).

Failure to Acquire

This document has described the three biometric tasks and their associated performance measures. However, there is another measure that may also be of interest because it affects all three biometric tasks. The Failure to Acquire rate is the rate at which a biometric system fails to capture and/or extract information from an observation. Numerous issues, including device/software malfunction, environmental concerns, and human anomalies (e.g., amputees not able to use hand geometry system, bricklayers with worn fingerprints, etc.), can cause a Failure to Acquire. For some biometric systems, or for certain applications, the Failure to Acquire rate could be quite high.

Different evaluations deal with this issue in different ways. Some (as in the examples above) force systems to produce similarity scores, even if there was a Failure to Acquire. This, of course, produces lower performance measures. Others only show performance (usually referred to as False Match Rates[a] and False Non-Match Rates[b]) on properly acquired signatures and show the Failure to Acquire rate separately. This, of course, raises the performance measures. Neither approach is wrong; evaluators simply choose the method that shows performance according to how the system will be used operationally. When reviewing others' evaluations, potential users will need to determine which approach was applied.

Other Performance Statistics

Other statistics are sometimes used to show performance of biometric systems. These, listed below, are defined in the accompanying Glossary.

- Crossover Error Rate (CER)
- Detection Error Trade-off (DET)
- Difference Score
- Equal Error Rate (EER)
- Failure to Enroll (FTE)
- False Match Rate
- False Non-Match Rate
- Hamming Distance
- Throughput Rate
- True Accept Rate
- True Reject Rate
- Type I Error
- Type II Error

Other Types of Testing

Not all biometric tests are accuracy-based. A summary of the more common of these tests is described below.

[a] The False Match Rate is equivalent to the False Acceptance Rate described in this paper.

[b] The False Non-Match Rate is similar to the False Reject Rate (FRR) described in this paper, except the FRR includes the Failure to Acquire error rate and the False Non-Match Rate does not.

Acceptance Testing: "The process of determining whether an implementation satisfies acceptance criteria and enables the user to determine whether or not to accept the implementation. This includes the planning and execution of several kinds of tests (e.g., functionality, quality, and speed performance testing) that demonstrate that the implementation satisfies the user requirements."[5]

Conformity: "Fulfillment by a product, process or service of specified requirements"*]*[6]

Conformity Evaluation: "Systematic examination of the extent to which a product, process or service fulfils specified requirements"[6]

Conformance Testing (or Conformity Testing): "Conformity evaluation by means of testing"[6]

Interoperability Testing: "The testing of one implementation (product, system) with another to establish that they can work together properly"[7]

Performance Testing: "Measures the performance characteristics of an Implementation Under Test (IUT) such as its throughput, responsiveness, etc., under various conditions"[5]

Robustness Testing: "The process of determining how well an implementation processes data which contains errors"[5]

Standards Activities

There are multi-part voluntary consensus standards for Biometric Performance Testing and Reporting under development by INCITS M1 and ISO/IEC JTC 1/SC 37. The first three parts of the INCITS American National Standard were approved by ANSI on October 25, 2005. These parts are:

INCITS 409.1-2005, American National Standard for Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework. This multipart standard develops a common set of methodologies and procedures to be followed for conducting technical performance testing and evaluations. Included are guidelines that address issues regarding required test sizes, performance statistics, error reporting, and presentation of performance results. These procedures

can be incorporated in an "end-to-end" system approach or from an individual technical component perspective.

INCITS 409.2-2005, American National Standard for Information Technology – Biometric Performance Testing and Reporting – Part 2: Technology Testing and Reporting. This standard specifies procedures for conducting offline tests of the performance of biometric technologies.

INCITS 409.3-2005, American National Standard for Information Technology – Biometric Performance Testing and Reporting – Part 3: Scenario Testing and Reporting. This standard specifies requirements for scenario-based biometric testing and reporting.

A similar standard is under development at the international level, ISO/IEC FDIS 19795-1:2005. Part 1: Principles and Framework is up for ballot. 19795-1 has been developed from the UK Biometrics Working Group's Best Practices in Testing and Reporting Performance of Biometric Devices. The UK document was developed from two NIST primary source documents developed by NIST, a variety of evaluation reports and input from the Biometric Consortium's Working Group on Interoperability, Performance and Assurance.

Important Items to Keep in Mind

There are two key items to keep in mind while reviewing biometric performance evaluation reports. First, not all evaluation results are relevant. If an evaluation report, particularly for a Scenario or Operational Evaluation, does not match the user's intended application, the usefulness of the results will be significantly diminished. Second, biometric evaluation results have a very limited shelf life. Researchers continue to make significant progress in improving the performance of a biometric system so if the report is more than 9-18 months old, the results should not be considered conclusive, but merely used as a general guide and reference.

Document References

[1] P. Philips, A. Martin, C. L. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems" (2000). <http://www.frvt.org/DLs/FERET7.pdf>.

[2] "Face Recognition Vendor Test," FRVT.org <http://www.frvt.org>.

[3] Tony Mansfield, Gavin Kelly, David Chandler, and Jan Kane, "Biometric Product Testing Final Report" 19 March 2001, CESG/BWG Biometric Test Programme http://www.cesg.gov.uk. <http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf>.

[4] P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone, "Face Recognition Vendor Test 2002" FRVT.org <http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf>.

[5] International Organization for Standardization, "Information technology -- JPEG 2000 image coding system: Conformance testing" ISO/IEC 15444-4:2004 <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39079&ICS1=35&ICS2=40&ICS3=&scopelist=>.

[6] International Organization for Standardization, "Standardization and related activities -- General vocabulary" ISO/IEC Guide 2:2004 <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39976>.

[7] National Institute of Standards and Technology, "Metrology for Information Technology (IT)" NISTIR 6025 <http://www.itl.nist.gov/lab/nistirs/ir6025.htm>.

About the Subcommittee

About the National Science and Technology Council

The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. Chaired by the President, the membership of the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

A primary objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in a broad array of areas spanning virtually all the mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across Federal agencies to form investment packages aimed at accomplishing multiple national goals. The work of the NSTC is organized under four primary committees; Science, Technology, Environment and Natural Resources and Homeland and National Security. Each of these committees oversees a number of sub-committees and interagency working groups focused on different aspects of science and technology and working to coordinate the various agencies across the federal government. Additional information is available at http://ostp.gov/nstc.

About the Subcommittee on Biometrics

Biometrics is a technology that is rapidly becoming a useful security, cost-savings and convenience tool for the Federal Government. Although the Federal Government is using the technology for many applications now, further development and assessment is required to improve the technology's utility. To address these issues, the Office of Science & Technology Policy (OSTP) created the NSTC Subcommittee on Biometrics, reporting to the National Science & Technology Council (NSTC) Committees on Technology and Homeland & National Security. Additional information is available at http://www.biometricscatalog.org/NSTCSubcommittee.

Subcommittee on Biometrics

Co-chair: Duane Blackburn (OSTP)

Co-chair: Chris Miles (DOJ)

Co-chair: Brad Wing (DHS)

Executive Secretary: Kim Shepard (FBI Contractor)

Department Leads

Mr. Jon Atkins (DOS)

Dr. Sankar Basu (NSF)

Mr. Duane Blackburn (EOP)

Ms. Zaida Candelario (Treasury)

Dr. Joseph Guzman (DoD)

Dr. Martin Herman (DOC)

Ms. Usha Karne (SSA)

Dr. Michael King (IC)

Mr. Chris Miles (DOJ)

Mr. David Temoshok (GSA)

Mr. Brad Wing (DHS)

Mr. Jim Zok (DOT)

Communications ICP Team

Champion: Kimberly Weissman (DHS US-VISIT)

Members & Support Staff:

Mr. Richard Bailey (NSA Contractor)

Mr. Duane Blackburn (OSTP)

Mr. Jeffrey Dunn (NSA)

Ms. Valerie Lively (DHS S&T)

Mr. John Mayer-Splain (DHS US-VISIT Contractor)

Ms. Susan Sexton (FAA)

Ms. Kim Shepard (FBI Contractor)

Mr. Scott Swann (FBI)

Mr. Brad Wing (DHS US-VISIT)

Mr. David Young (FAA)

Mr. Jim Zok (DOT)

Special Acknowledgements

The Communications ICP Team wishes to thank the following external contributors who provided assistance on one or more documents:

- Joseph (Mike) Bone
- Jim Cambier
- Dirk Colbry
- FBI CJIS Division
- FBI Laboratory Division
- Fingerprint Recognition ICP Team
- Ed German
- Peter Higgins
- Mike Hogan
- IBIA
- Rick Lazerick
- Dave Lohman
- James Matey
- Stephen Meagher
- Hirotaka Nakasone
- Nick Orlans
- Donald Reynolds
- Arun Ross,
- Kelly Smith
- Ron Smith
- Standards ICP Team
- B. Scott Swann
- Dr. Kathryn Taylor
- Test and Evaluation ICP Team
- Jim Wayman

Document Source

This document, and others developed by the NSTC Subcommittee on Biometrics, can be found at http://www.biometricscatalog.org/NSTCSubcommittee.